NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: **All Actions**	**Civil Action No. 19-md-2904** **OPINION**

ARLEO, UNITED STATES DISTRICT JUDGE

THIS MATTER comes before the Court by way of motions to dismiss five Consolidated Class Actions Complaints (the "CCACs") filed in connection with the instant multidistrict litigation ("MDL"). For the reasons set forth below, the Motions are **GRANTED IN PART** and **DENIED IN PART**.

This MDL arises from a data breach suffered by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency ("AMCA"). Defendants are primarily healthcare providers who hired AMCA as a collections vendor and provided AMCA with sensitive patient information to facilitate collections. Between late 2018 and March 2019, an unauthorized user or users gained access to an AMCA computer system containing the private information of millions of patients (the "Data Breach"). Plaintiffs are among those patients whose personal information was impacted by the Data Breach. Each CCAC alleges claims against a different defendant or group of defendants.[1]

[1] CCACs have been filed against (1) Quest Diagnostics Inc. ("Quest") and Quest's revenue services vendor, Optum360 LLC ("Optum360"), see ECF No. 104 (the "Quest CCAC"); (2) Laboratory Corporation of America Holdings ("LabCorp"), see ECF No. 105 (the "LabCorp CCAC"); (3) Sonic Healthcare USA ("Sonic USA") and its subsidiaries (the "Sonic Subsidiaries" and together with Sonic USA, "Sonic"), see ECF No. 107 (the "Sonic CCAC"); (4) CareCentrix, Inc. ("CareCentrix"), see ECF No. 133 (the "CareCentrix CCAC"); and (5) Inform Diagnostics, Inc. ("Inform"), see ECF No. 193 (the "Inform CCAC").

This Opinion resolves Defendants' respective motions to dismiss the CCACs.[2]

I. Factual Background

A. Defendants' Collection of Personal Information

Quest, LabCorp, Sonic, and Inform are providers of medical diagnostic services including, among other things, blood testing, urinalysis, and biopsies. Quest CCAC ¶¶ 302-03; LabCorp CCAC ¶¶ 44-46; Sonic CCAC ¶ 65, 76-82; Inform CCAC ¶ 24. CareCentrix (together with Quest, LabCorp, Sonic, and Inform, the "Healthcare Defendants") provides "health benefits management services" by connecting patients with healthcare providers throughout the country. CareCentrix CCAC ¶ 45.

Patients must pay for the services rendered by the Healthcare Defendants, either through insurance or out of pocket. See, e.g., Quest CCAC ¶ 305.[3] To facilitate medical care and billing, the Healthcare Defendants collect and maintain personal information from their patients, including names, mailing addresses, phone numbers, email addresses, dates of birth, Social Security numbers, genders, and medical information, credit and debit card numbers, bank accounts, and insurance information (collectively, "Personal Information"). See, e.g., id. ¶ 4.

B. The Data Breach

When a patient failed to pay an invoice within a specified time, the Healthcare Defendants would refer the matter to AMCA for collections. See, e.g., Quest CCAC ¶ 306. LabCorp, Sonic,

[2] This Opinion concerns the following motions presently pending before the Court: (1) Sonic's Motion to Dismiss the Sonic CCAC, ECF No. 147; (2) LabCorp's Motion to Dismiss the LabCorp CCAC pursuant to Rules 12(b)(1) and 12(b)(6), ECF No. 148; (3) Optum360's Motion to Dismiss the Quest CCAC, ECF No. 149; (4) Quest's Motion to Dismiss the Quest CCAC, ECF No. 150; (5) CareCentrix's Motion to Dismiss the CareCentrix CCAC, ECF No. 176; and (6) Inform's Motion to Dismiss the Inform CCAC, ECF No. 213 (collectively the "Motions"). The Court will independently address LabCorp's separately filed Partial Motion to Dismiss the LabCorp CCAC for lack of personal jurisdiction pursuant to Rule 12(b)(2), ECF No. 146.

[3] Plaintiffs make substantially similar allegations in each CCAC. The Court primarily refers to allegations in the Quest CCAC, except where necessary to distinguish between the pleadings.

Carecentrix, and Inform each contracted directly with AMCA, as did Quest prior to September 2016. Quest CCAC ¶ 306; LabCorp CCAC ¶ 52; Sonic CCAC ¶ 84; CareCentrix CCAC ¶ 47; Inform CCAC ¶ 26. In September 2016, Quest outsourced its revenue services operations to Optum360 (together with the Healthcare Defendants, "Defendants") and assigned its contract with AMCA to Optum360. Quest CCAC ¶ 306.

Defendants supplied AMCA with their patients' Personal Information when referring an invoice for collections. See, e.g., Quest CCAC ¶ 307.[4] Some patients also furnished Personal Information directly to AMCA. See, e.g., id. ¶ 309. AMCA then stored the Personal Information on its computer systems. Id. ¶ 307.[5]

Between August 1, 2018 and March 2019, an unidentified user or users gained access to an AMCA system that contained the Personal Information of Defendants' patients. See, e.g., id. ¶ 310.[6] On February 28, 2019, nonparty Gemini Advisory ("Gemini") identified several compromised payment cards for sale while monitoring dark-web marketplaces. Id. ¶ 312. Gemini conducted an analysis, which concluded that the information was likely stolen from AMCA's online portal. Id. Several financial institutions also allegedly confirmed the connection between the payment card data and the Data Breach. Id. Gemini attempted to notify AMCA on March 1, 2019, but received no response. Id. ¶ 314. Gemini then contacted law enforcement, who followed

[4] Plaintiffs allege that notwithstanding the assignment to Optum360 in September 2016, Quest continued to supply its patients' Personal Information to AMCA, either directly or through Optum360. Quest CCAC ¶¶ 306-07

[5] In a public bankruptcy filing, AMCA acknowledged that it maintained data transmitted by its clients, including patients' names, dates of birth, home addresses, social security numbers, bank account information, and credit card information. See Quest CCAC ¶ 308.

[6] The Data Breach allegedly impacted more than 22 million of Defendants' patients. See Quest CCAC ¶ 310; LabCorp CCAC ¶ 59; Sonic CCAC ¶ 88; CareCentrix CCAC ¶ 40; Inform CCAC ¶ 19.

up with AMCA. Id. After notification from law enforcement, AMCA's payment portal became unavailable. Id. ¶ 315.[7]

On May 14, 2019, AMCA notified Quest and LabCorp of the Data Breach. Id. ¶ 310; LabCorp CCAC ¶ 63. AMCA also notified Sonic, CareCentrix, and Inform in May 2019. Sonic CCAC ¶ 95; CareCentrix CCAC ¶ 70; Inform CCAC ¶ 44. Thereafter, AMCA filed for Chapter 11 bankruptcy on June 17, 2019, in the Southern District of New York. See Quest CCAC ¶ 318.

C. Defendants' Notice to Customers

The CCACs generally allege that Defendants failed to provide sufficient notice of the Data Breach to their customers. Quest and Optum360 first publicly announced the breach in a June 3, 2019 SEC filing. Quest CCAC ¶¶ 310, 334. LabCorp followed suit the next day in a public filing dated June 4, 2019. LabCorp CCAC ¶¶ 65-67, 81.[8] During the month of June 2019, neither Quest nor LabCorp sent notices directly to their patients; rather they allegedly relied on AMCA to notice the effected individuals. Quest CCAC ¶ 336; LabCorp ¶ 83. Beginning in July 2019, LabCorp and Quest put detailed information regarding the Data Breach on their websites and began sending personal notices to impacted customers. Quest CCAC ¶¶ 337-38; LabCorp CCAC ¶¶ 84-85.

Sonic first publicly acknowledged the Data Breach in mid-July 2019. Sonic CCAC ¶ 99. Plaintiffs allege that Sonic never sent direct notice to many of its impacted patients. Id. ¶¶ 99-100. CareCentrix and Inform allegedly began notifying patients of the Data Breach in July 2019. CareCentrix CCAC ¶ 49; Inform CCAC ¶ 28.

---

[7] AMCA allegedly learned of the breach on March 20, 2019. See Quest CCAC ¶ 316.

[8] LabCorp's June 4, 2019 further noted that "AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers." LabCorp CCAC ¶ 68. In a subsequent August 8, 2019 filing, LabCorp advised that social security numbers and health insurance information may also have been compromised. Id. ¶¶ 68-69

D. The Alleged Warning Signs

The CCACs further allege that Defendants failed to take proper care to protect their patients' Personal Information from the Data Breach. As early as 2014, the FBI alerted the healthcare industry that it was a preferred target of hackers and urged healthcare companies to take precautions. See. e.g., Quest CCAC ¶ 359. Plaintiffs also assert that the healthcare industry is generally known amongst security experts to be susceptible to data breaches due to its common use of personally identifying information, which is a valuable commodity on the black market. Id. ¶¶ 360, 362-65. As of the end of 2018, the healthcare sector allegedly had the second-highest number of data breaches among measured sectors. Id. ¶ 361.[9]

Given this background, Plaintiffs maintain that Defendants did not employ industry-standard safeguards to investigate AMCA before supplying Personal Information or to monitor AMCA during their relationships. In this regard, Plaintiffs assert that (1) AMCA was thinly capitalized, allegedly demonstrated by the fact that its owner needed to take out a personal loan to acquire the funds needed to mail notices to impacted customers; (2) AMCA never detected the Data Breach on its own, ostensibly showing a gap in its security capabilities; (3) Defendants did not ensure AMCA maintained appropriate procedures for encrypting, destroying, and archiving Personal Information; and (4) Defendants each failed to learn about the Data Breach until two months after AMCA learned of it. See, e.g., Quest CCAC ¶¶ 327-33.

[9] Plaintiffs further allege that LabCorp, CareCentrix, and a Sonic Subsidiary each suffered minor information security breaches in the past, although none under circumstances similar to the instant Data Breach. See LabCorp CCAC ¶ 113; CareCentrix CCAC ¶ 94; Sonic CCAC ¶ 138.

E. The Named Plaintiffs[10]

The Court identifies three broad groups of patients who allege that their Personal Information was transmitted to AMCA during the relevant period, distinguished by their alleged injuries. The first group consists of patients who have allegedly suffered economic injuries resulting from the misuse of Personal Information stolen in the Data Breach, regardless of whether any out-of-pocket injuries were ultimately reimbursed (the "Group I Plaintiffs"). Such injuries primarily consist of fraudulent charges on credit cards or bank accounts, as well as the cost of any measures taken to resolve the fraudulent charges. See, e.g., Quest CCAC ¶¶ 28-29, 156-61; LabCorp CCAC ¶¶ 11-13.[11]

The second group includes patients who have not experienced direct economic harm, but who have alleged facts sufficient to infer that an unauthorized user obtained the patient's Personal Information in the Data Breach (the Group II Plaintiffs"). For example, some plaintiffs allege that unknown parties unsuccessfully attempted to misuse their financial information. See, e.g., Quest CCAC ¶¶ 51, 233; LabCorp CCAC ¶¶ 21, 28.[12]

The final group is comprised of the remaining plaintiffs, i.e., those patients who allege that their Personal Information was stored in the compromised AMCA systems but do not allege any

---

[10] Throughout this Opinion, the Court refers to plaintiffs asserting claims against Quest and Optum360 as the "Quest Plaintiffs," plaintiffs asserting claims against LabCorp as the "LabCorp Plaintiffs," and so forth.

[11] Group I consists of (a) 4 Quest Plaintiffs: (i) Julio Antonio Perez Vieyra, (ii) Elizabeth Hollway, (iii) Ria Jairam, and (iv) Ann Davis; and (b) 9 LabCorp Plaintiffs: (i) Sherrie Palmer, (ii) Sandra Lassiter, (iii) Aleksander Nazemnikov, (iv) Tanya Harris, (v) Holly Laufenberg, (vi) Tatyana Shulman, (vii) Kristopher Thomas, (viii) Rosaria Gadero, and (ix) Melanie Vazquez.

[12] Group II consists of (a) 6 Quest Plaintiffs: (i) Noel Benadom (attempted charge), (ii) Nancy Infield (phishing calls), (iii) Michael Rutan (increased mailings and robocalls), (iv) John Briley (attempted account opening), (v) Joyce Rosselli (email for sale on "dark web"), and (vi) Darlane Saracina (social security number for sale on "dark web"); (b) 8 LabCorp Plaintiffs: (i) Timothy Petri (personal information on cellphone accessed and deleted), (ii) Valerie Scott (attempted charges), (iii) Cameron Spencer (unauthorized credit inquiries), (iv) Lori Lamondie-Murphy (attempted account openings), (v) Debra Wrenn (unauthorized credit inquiry), (vi) Edith Thrower (unauthorized credit inquiries), (vii) Timothy Judelsohn (credit card "cloned" without authorization), and (viii) Tiffany Goins (unauthorized credit inquiry); and (c) 2 Sonic Plaintiffs: (i) Gwendolyn Anderson (unauthorized user accessed several web accounts) and (ii) Daniel Davis (attempted fraudulent withdrawal from bank account).

other facts to suggest that their information was actually accessed, downloaded, or misused by an unauthorized party (the "Group III Plaintiffs").[13] Most of these plaintiffs were informed that their information was at risk, and some allege that they took prophylactic measures to protect themselves from identity theft. See, e.g., Quest CCAC ¶¶ 39-40, 98-100; LabCorp CCAC ¶¶ 14-15.

Each Plaintiff contends that their asserted injuries were caused by the Data Breach and Defendants' failure to secure their Personal Information. See, e.g., Quest CCAC ¶ 428.

II. PROCEDURAL HISTORY

On July 31, 2019, the United Stated Judicial Panel on Multidistrict Litigation ("JPML") initiated the instant MDL pursuant to 28 U.S.C. § 1407(a). ECF No. 1. The JPML initially transferred and consolidated ten actions after finding that they each presented "common factual questions concerning [the Data Breach]" including:

> (1) AMCA's data security practices and whether they met industry standards; (2) how the unauthorized access occurred; (3) when defendants knew or should have known of the breach; (4) the investigation into the breach; and (5) the alleged delay in disclosure of the breach by all defendants.

Id. at 3. Since the initial Transfer Order, additional tag-along actions have been transferred or directly filed into the MDL.

Plaintiffs thereafter filed the CCACs, which consolidated the individual claims of many plaintiffs who had previously filed claims in districts throughout the country and added additional

[13] Group III consists of (a) 17 Quest Plaintiffs: (i) Ella Gulley, (ii) Moises Perez, (iii) William Infield, (iv) Annie Mae Smith, (v) Shannon Walden, (vi) Lucinda Dirks, (vii) Ashley Finch, (viii) Carolyn Green, (ix) Rose Marie Perry, (x) LaTease Rikard, (xi) Naomi Jaworowski, (xii) Cynthia Connor; (xiii) Karli Parker, (xiv) Deanna Taylor, (xv) William Lindsay, (xvi) Brittney Petitta, and (xvii) Jo Ann Buck; (b) 15 LabCorp Plaintiffs: (i) Tracy Buhr, (ii) Susan Duckworth, (iii) Jennifer Haley, (iv) Justin Nelson-Carter, (v) David Finch, (vi) George Rothwell, (vii) Cassandra Jerry, (viii) Carol Kaplan, (ix) Brenda Evans, (x) Jesse Lebon, (xi) Wendy Wallach, (xii) Sheera Harris, (xiii) Isaac Williams-Winders, (xiv) Martha Cuviller, and (xv) Gina Allende; (c) 2 Sonic Plaintiffs: (i) Tim Collinsworth and (ii) Tonda Tate; (d) 3 CareCentrix Plaintiffs: (i) Brian Graifman, (ii) Debbie Amico, and (iii) L.D.; and (e) 1 Inform Plaintiff: Pernell Thomas.

plaintiffs who had not previously asserted claims. Collectively, the CCACs raise the claims of 67 named plaintiffs under the common law, consumer fraud statutes, and data breach statutes of over twenty states. The CCACs further assert the claims of putative nationwide and statewide classes consisting of "[a]ll natural persons . . . whose Personal Information was compromised in the Data Breach." See e.g., Quest CCAC ¶ 387.

Defendants now move to dismiss the CCACs in their entirety for lack of subject-matter jurisdiction and failure to state a claim upon which relief can be granted.

III. Legal Standard

A. Rule 12(b)(1)

In resolving a Rule 12(b)(1) motion, a court first determines whether the motion presents a "facial" or "factual" attack on subject matter jurisdiction. See Const. Party of Pa. v. Aichele, 757 F.3d 347, 357 (3d Cir. 2014). A facial attack argues that a claim on its face "is insufficient to invoke the subject matter jurisdiction of the court," id. at 358, and does not dispute the facts alleged in the complaint, Davis v. Wells Fargo, 824 F.3d 333, 346 (3d Cir. 2016). A court reviewing a facial attack must "consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." Const. Party of Pa., 757 F.3d at 358. Here, the Motions present facial attacks because they assert, based solely on the Complaint, that Plaintiffs lack Article III standing. See, e.g., Quest Mem. at 11-23, ECF No. 150.1.

B. Rule 12(b)(6)

In resolving a Rule 12(b)(6) motion to dismiss, the Court accepts all pleaded facts as true, construes the complaint in the plaintiff's favor, and determines "whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief." Phillips v. County of Allegheny, 515 F.3d 224, 233 (3d Cir. 2008) (internal quotation marks and citation omitted). To survive a

motion to dismiss, the claims must be facially plausible, meaning that the pleaded facts "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). The allegations must be "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007).

IV. ANALYSIS

Defendants first argue that Plaintiffs lack Article III standing to pursue their respective claims in federal court. They also contend that each of Plaintiffs' many substantive claims fail as a matter of law and must be dismissed for failure to state a claim upon which relief can be granted. The Court first assesses Plaintiffs' standing before addressing the merits of Plaintiffs' claims under state common law, consumer protection statutes, and cybersecurity statutes.

A. Article III Standing

Plaintiffs each allege that AMCA possessed their respective Personal Information at the time of the Data Breach. Most Plaintiffs further allege that he or she was informed that such Personal Information may have been "compromised" or "at risk." Yet only some Plaintiffs have plausibly alleged facts from which the Court may infer that their information was demonstrably accessed, disseminated, or misused by hackers, and even fewer allege they have suffered financial harm because of the Data Breach.

Article III limits federal courts' jurisdiction to actual "cases or controversies." U.S. Const. art. III. § 2. This requirement places the burden on Plaintiffs to establish their "standing to sue." Raines v. Byrd., 521 U.S. 811, 818 (1997). At the pleading stage, Article III requires a plaintiff to allege facts showing (1) an "injury in fact;" (2) a causal connection between that injury and the conduct complained of; and (3) that such injury will likely be "redressed by a favorable decision."

Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992). Each named plaintiff in a class action must personally demonstrate standing independently of any claims brought on behalf of a putative class. See Lewis v. Casey, 518 U.S. 343, 357 (1996).

Defendants argue that Plaintiffs have failed to establish the injury and causation requirements necessary to establish Article III standing. The Court addresses each element in turn.

1. Injury-in-Fact

The injury-in-fact requirement contains two core components. First, an alleged injury must be "concrete in both a qualitative and temporal sense." Reilly v. Cerdian Corp., 664 F.3d 38 (3rd Cir. 2011) (quoting Whitmore v. Arkansas, 495 U.S. 149, 155 (1990)). More specifically, a plaintiff "must allege an injury to himself that is 'distinct and palpable,' as distinguished from merely 'abstract,' and the alleged harm must be actual or imminent, not 'conjectural or 'hypothetical.'" Id.; see also Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016). Second, an injury must be "particularized," in that it "affect[s] the plaintiff in a personal and individual way." Lujan, 504 U.S. at 561 n.1.

"[C]ertain harms readily qualify as concrete injuries under Article III. The most obvious are traditional tangible harms, such as physical harms and monetary harms." TransUnion v. Ramirez, 141 S. Ct. 2190, 2204 (2021). However, even intangible harms that are hard to quantify can be sufficiently "concrete" to establish an injury-in-fact. The Supreme Court recently explained that to determine whether an intangible harm presents a constitutionally recognized injury, federal courts must analyze whether an alleged harm bears a "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." Id.; see also Spokeo, 578 U.S. at 341.

In TransUnion, the Court considered whether a class of plaintiffs whose credit reports were misleadingly marked as presenting a risk by the Officer of Foreign Assets Control ("OFAC") had suffered an Article III injury. The Court held that the 1,853 class members whose credit reports were disseminated to third-party businesses with misleading information—though they did not necessarily suffer direct economic injury—had suffered a harm that bore a "close relationship" to the reputational harm associated with the tort of defamation. TransUnion, 141 S.Ct. at 2208. On the other hand, the Court found that the remaining 6,332 class members did not suffer an injury because although their credit files contained misleading information, the misleading OFAC alert was not sent to a third-party. The Court again analogized to defamation and reasoned that because "[p]ublication is 'essential to liability' in a suit for defamation," those plaintiffs' failure to establish that the misleading alert was transmitted precluded standing. Id. The Court rejected the argument that the mere existence of the misleading credit file was itself sufficient for injury because of the hypothetical risk that it could be sent to third-parties in the future. Absent factual support that this risk "materialized," the remaining plaintiffs failed to establish standing. Id. at 2212. Thus, the Supreme Court's decision in TransUnion reaffirms that a "mere risk of future harm," divorced from actual harm, is insufficient to support standing in a suit for damages. Id.

Given the intangible harms inherent in having one's personal information compromised, plaintiffs in information security and data privacy cases raise unique issues with respect to standing. Generally, a plaintiff in a data breach case can establish standing through allegations tending to show that his or her individual information has actually been accessed, disseminated, or misused by an unauthorized party. See, e.g., In re Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017). On the other hand, speculation that a plaintiff's data "may have been accessed" in a large data breach is insufficient. Reilly, 664 F.3d at 43. In Reilly,

the Third Circuit[14] considered whether plaintiffs suffered an injury when an unknown third-party wrongfully accessed a server containing their electronically-stored information, but no facts suggested the third party had read, copied, understood, or used that information. Id. at 42. The court decisively answered that question in the negative, reasoning that "[a]llegations of possible future injury are not sufficient to satisfy Article III." Reilly, 664 F.3d at 42 (finding no standing based on the "indefinite risk of future harms inflicted by unknown third parties"). In other words, the fact that some plaintiffs' Personal Information may have been accessed and misused does not necessarily create a particularized injury as to all Plaintiffs whose data was in AMCA's possession. See In re Horizon, 846 F.3d at 641 n.22 (explaining that the "particularization requirement may impose limits on the ability of consumers to bring suit" based on "generalized grievances"); cf. TransUnion, 141 S. Ct. at 2208, 2212.

Still, once a plaintiff satisfies her burden to allege facts suggesting the actual dissemination of her personal information, she may establish standing without an additional showing of direct economic injury. Indeed, when it comes to "laws that protect privacy, a focus on economic loss is misplaced." In re Horizon, 846 F.3d at 636 (citation and internal quotation marks omitted). Rather, the unauthorized disclosure of personal information itself constitutes "a clear de facto injury." Id. In In re Horizon, the Third Circuit held that because privacy torts at common law recognize improper dissemination as a cognizable injury, "the unauthorized dissemination of personal information" causes "an injury in and of itself—whether or not the disclosure of that information increase[s] the risk of identity theft or some other future harm." Id. at 639.

---

[14] "On issues of federal law or federal procedure, the MDL transferee court applies the law of the circuit in which it sits (here, the Third Circuit)." In re Asbestos Prod. Liab. Litig. (No. VI), 965 F. Supp. 2d 612, 616 (E.D. Pa. 2013); see also In re Plavix Mktg., Sales Prac. & Prod. Liab. Litig. (No. II), 332 F. Supp. 3d 927, 936 (D.N.J. 2017) ("The law of the transferee forum applies . . . to federal questions").

As discussed, the Court identifies three distinct groups of plaintiffs who allege myriad harms resulting from the Data Breach. See supra Section I.E. The Court must individually analyze the unique injuries asserted by each group to determine whether each plaintiff has alleged a concrete and particularized injury.

a. Group I Plaintiffs

The Group I Plaintiffs have plausibly alleged economic injuries resulting from the Data Breach. In turn, the Court finds that they have adequately alleged an injury-in-fact.

The alleged economic harms are quintessentially concrete. For example, Quest Plaintiff Hollway[15] alleges she experienced several fraudulent charges on her financial accounts and a fraudulent account opened in her name. Quest CCAC ¶¶ 156-60.[16] LabCorp Plaintiffs Nazemnikov, T. Harris, and Laufenburg likewise allege having experienced "several" fraudulent charges on their credit or debit cards. LabCorp CCAC ¶¶ 13, 16-17. These plaintiffs also allege that, in addition to fraudulent charges, they suffered subsequent economic injury because they invested time and money into combating and mitigating these manifestations of identity theft. See, e.g., Quest CCAC ¶¶ 156-60; Lab Corp CCAC ¶¶ 13, 16-17.

Defendants argue that "Plaintiffs who allege they discovered unauthorized charges on payment cards or in bank accounts" fail to allege an injury-in-fact because they "do not allege that they had to pay for any fraudulent charge." LabCorp Mem. at 10, ECF No. 148.1 (emphasis added); see also Quest Mem. at 15 (arguing fraudulent charges must be "unreimbursed" to establish injury). This is incorrect. That some Plaintiffs may have been able to remedy some of

[15] The Court hereafter refers to individual Plaintiffs by their respective surnames.

[16] Quest and Optum concede that Hollway suffered a concrete injury but dispute standing on other grounds. Quest Mem. at 10 n.7; Optum Mem. at 8 n.5. They make no similar concessions with respect to other Plaintiffs who suffered fraudulent charges, including Perez-Vieyra, Quest CCAC ¶ 29, Jairam, id. ¶ 189, and Davis, id. ¶ 294.

the fraudulent charges they suffered does not mean they did not suffer economic injury. As an initial matter, it is a misreading of the applicable case law to assert that only "unreimbursed" financial charges confer actionable injury. See In re Horizon, 846 F.3d at 638-39. The fraudulent charges identified by the Group I Plaintiffs permit the inference that their specific information has been accessed and misused. Therefore, at a minimum, they have suffered the actionable intangible harm of the wrongful use and dissemination of their private information, like the interests protected by common law privacy torts. See TransUnion, 141 S. Ct. at 2208.

Moreover, the Group I Plaintiffs allege they incurred expenses in addressing and resolving these charges to mitigate their injury—in turn they have suffered further economic injury attributable to the Data Breach. See, e.g., Quest CCAC ¶¶ 156-60; LabCorp CCAC ¶¶ 13, 16-17. While a plaintiff cannot establish standing through prophylactic expenses incurred in an attempt to stave off hypothetical harm, Reilly, 664 F.3d at 46, remedial expenses are sufficiently concrete when the harm a plaintiff faces has already "materialized," TransUnion, 141 S. Ct. at 2211; see e.g., Anderson v. Hannaford Bros. Co., 659 F.3d 151, 164-67 (1st Cir. 2011) (holding that the "costs of credit monitoring services and identity theft insurance" are cognizable injuries when incurred by plaintiffs who had already suffered fraudulent charges to their accounts and thus had a reasonable basis to incur expenses to prevent further harm).[17]

Plaintiffs that have been the victim of fraud and identity theft face a corroborated risk that they could suffer the same harm again. This factor distinguishes the remedial expenses incurred by the Group I Plaintiffs—incurred in reasonable response to a manifestation of past identity

[17] To be clear, the issue is not whether credit monitoring and related expenditures are concrete economic losses; manifestly, they are. Rather, the Court must ask whether such voluntary expenses can fairly be considered "injuries" attributed to Defendants' conduct. Cf. Reilly, 664 F.3d at 46 ("[C]osts incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than [an] alleged 'increased risk of injury.'").

theft—from the prophylactic measures found insufficient in Reilly, which were based solely on a highly speculative and uncorroborated fear of future identity theft. See Anderson, 659 F.3d at 164-65; see also F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 623-24 (D.N.J. 2014) (finding Reilly inapplicable when there is an allegation of misuse).

Therefore, the Court finds that the Group I Plaintiffs have suffered concrete and particularized economic injuries arising from fraudulent charges and remedial measures taken to resolve charges and prevent further fraud.

b. Group II Plaintiffs

The Group II Plaintiffs allege solely intangible harms but plead facts suggesting that their individual private information was wrongfully accessed and distributed. Defendants argue that such disclosure is not an "actual[] harm[]" sufficient to confer standing without allegations that the information was used to Plaintiffs' detriment. E.g., LabCorp. Mem. at 10. The Court disagrees.

These Plaintiffs allege that their Personal Information has been misused in numerous ways, including foiled attempts at identity theft, an increase in scam phone calls, and the sale of Personal Information on the dark web. The precise facts they allege are diverse. For example, Plaintiff Benadom alleges a third-party "attempted" to book a $125 ticket to Universal Studios on Orbitz.com using her information. Quest CCAC ¶ 52. Plaintiff Briley alleges that an imposter attempted to open a "Samsung Financing" account using a false name and his mailing address, but the application was denied. Id. ¶ 210. Plaintiff Rosselli alleges her email address was posted on the "dark web," id. ¶ 233, and Plaintiff Petri alleges his personal email address and website were all-together erased and made inaccessible, LabCorp CCAC ¶ 18. The specific nature of the injuries these plaintiffs experienced differ, but they share a critical similarity: they all have identified some corroboration that their Personal Information was accessed.

Drawing all inferences in favor of the Group II Plaintiffs, their allegations adequately plead an injury-in-fact. Again, intangible harms are sufficiently "concrete" to establish an injury-in-fact where they share a "close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." TransUnion, 141 S. Ct. at 2204. An unauthorized "disclosure of private information" is among these harms. Id.; Morales v. Healthcare Revenue Recovery Grp., LLC, 859 F. App'x 625, 628 (3d Cir. 2021) ("Disclosing 'personal information' is a concrete injury.") (quoting In re Horizon, 846 F.3d at 629); see also Restatement (Second) of Torts § 652A (2016) ("One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other."); Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 462 (7th Cir. 2020) ("The common law has long recognized actions at law against defendants who invaded the private solitude of another by committing the tort of 'intrusion upon seclusion.'") (cited approvingly in TransUnion).

A plaintiff who suffers a wrongful disclosure need not additionally demonstrate misuse resulting in economic harm. For example, the named-plaintiffs in TransUnion did not allege direct economic harm beyond the dissemination of the misleading OFAC alert. See TransUnion, 141 S.Ct. at 2201 (explaining that, despite receiving an alert, the car dealer nonetheless sold the car to plaintiff's wife). Here, the Group II Plaintiffs allege facts that suggest their Personal Information has been accessed and manipulated by hackers and third-parties following a data breach. By alleging these facts, the Group II Plaintiffs have pled an injury to their privacy interests, and Article III allows them to seek relief for that harm. Morales, 859 F. App'x at 628. That the wrongdoers were ultimately unsuccessful at using this data to Plaintiffs' financial ruin does not change this conclusion.[18]

[18] Moreover, the some of the Group II Plaintiffs allege that their Personal Information was used to run unauthorized credit inquiries, resulting in "lowered credit scores." See LabCorp CCAC ¶¶ 28, 35, 37, 40, 124(f). Courts have

The Court finds that the Group II Plaintiffs have each plausibly alleged a concrete and particularized intangible injury arising from the intrusion upon their privacy interests following the alleged wrongful access and misuse of their Personal Information.

c. Group III Plaintiffs

Group III includes the many Plaintiffs that have alleged no facts to support an inference that their particular information was accessed, stolen, or misused. They seek to establish an Article III injury based on (1) an increased risk of future identity theft; (2) expenses incurred to prevent future identity theft; (3) the allegedly diminished value of their Personal Information; and (4) a lost "benefit of the bargain" regarding the services purchased from Defendants. None of these provides a sufficient injury-in-fact.

First, each Plaintiff alleges that he or she incurred expenses to prevent future identity theft following notice of the Data Breach. See, e.g., Quest CCAC ¶ 33; LabCorp CCAC ¶ 14. But unlike the Groups I and II Plaintiffs, the Group III Plaintiffs have not alleged that they were the victims of past identity theft, nor have they pled any other particularized facts that would corroborate a fear of identity theft. This is the type of speculative harm that the Third Circuit squarely rejected in Reilly, 664 F.3d at 46. Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 416 (2013).

Second, Plaintiffs argue that they face a substantial risk of future harm because "criminals are committing fraud" with information stolen from the Data Breach. Pl. Opp. to Quest Mot. at 7, ECF No. 166. Plaintiffs assert that because some among them have been victimized by

recognized that a reduced credit score independently constitutes a concrete injury even without direct economic consequences. See, e.g., Boone v. T-Mobile USA Inc., No. 17-378, 2018 WL 588927, at *8-9 (D.N.J. Jan. 29, 2018) (collecting cases).

cyber-crime, that all of them run a substantial risk of falling victim to some cyber-crime or fraud. However, that others have suffered some concrete injury following the Data Breach is insufficient to establish the particularized reasonableness of these plaintiffs' fears of future harm. Plaintiffs cite, inter alia, In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 58 (D.C. Cir. 2019) and In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig., 440 F. Supp. 3d 447 (D. Md. 2020) ("In re Marriott"), in support of their position. However, while these out-of-circuit cases may suggest that a plaintiff need not always "wait until they . . . suffer identity theft to bring their claims," In re Marriott, 440 F. Supp. 3d at 460, they fail to account for the Third Circuit's binding decision in Reilly considering these precise facts, or the Supreme Court's recent admonition that an unmaterialized risk of future of harm cannot confer standing in a claim for damages, TransUnion, 141 S. Ct. at 2211. Absent some particularized harm to substantiate the Group III Plaintiffs' fears, their alleged injury is simply too conjectural. And "[u]nless and until these conjectures come true, [these Plaintiffs] have not suffered any injury." Reilly, 664 F.3d at 42.[19]

Third, Plaintiffs further attempt to prop up their standing argument on the theory that the Data Breach has diminished the "value" of their Personal Information. Plaintiffs assert that they may recover for any decline in the value of their Personal Information irrespective of whether they intended to sell or monetize that information. In support, Plaintiffs cite Marriott for the proposition that "the growing trend across courts that have considered this issue is to recognize the lost property value of [their] information." 440 F. Supp. 3d at 460-61. As a threshold matter, this

[19] The Court notes that a plaintiff may sometimes establish standing to pursue injunctive relief to protect against imminent future harm. See Clapper, 568 U.S. at 420; see also TransUnion 141 S.Ct. at 2210 ("[A] person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial."). The Parties have not briefed this issue in the context of Article III standing. Nonetheless, the Court concludes that Plaintiffs have failed to allege a threat of redressable future harm, for the reasons discussed in Section IV.D.3, infra. Thus, the Group III Plaintiffs' claims for injunctive relief are insufficient to establish standing.

theory suffers from the same deficiency as the others: without particularized allegations the Group III Plaintiffs' Personal Information were actually accessed or misused, these plaintiffs cannot plausibly allege that their information suffered any decrease in value.

Moreover, Plaintiffs' reliance on In re Marriott is misplaced. In re Marriott, like other courts adopting this theory of injury, involved circumstances where the defendants collected information that was itself monetized and used for commercial purposes. Id. at *8. The plaintiffs therein provided their information, and Marriott collected it "to better target customers and increase its profits" and "pa[id] a customer analytics company to analyze personal information for this purpose." Id. The CCACs here contain no similar allegation. Absent such circumstances, there is no loss of value in the information sufficient to state a concrete injury. Cf. In re Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 148 (3d Cir. 2015) (finding plaintiffs failed to allege a "loss" under the Computer Fraud and Abuse Act absent allegations they "participated or intended to participate in the market [for their electronic information]").[20]

Fourth and finally, Plaintiffs contend that they have suffered an economic injury based on an alleged decrease in the value of the services they received from Defendants. Specifically, certain Plaintiffs allege that they failed to get the "benefit of their bargain," in light of the Data Breach. See, e.g., Quest CCAC ¶ 572. This argument is without merit. The CCACs lack any allegation that Plaintiffs' Personal Information was of any material economic value with respect to the services Plaintiffs received from Defendants. Cf. In re Brinker Data Incident Litig., No. 18-686, 2020 WL 691848, at *13 (M.D. Fla. Jan. 27, 2020) ("In re Brinker") (rejecting "benefit of

[20] The Third Circuit held that the plaintiffs in In re Google had standing because they "base[d] their claims on highly specific allegations that the defendants, in the course of serving advertisements to their personal web browsers, implanted tracking cookies on their personal computers." 806 F.3d at 134. For the reasons discussed above, the Court finds the generalized allegations in the CCACs as to the Group III Plaintiffs are distinguishable because they lack the requisite concreteness and particularity.

the bargain" theory alleging that defendants failed to protect financial information plaintiffs supplied to purchase food and drinks because "the food or drink purchased ha[d] no diminished value because of [defendant's] alleged inadequate data security"). And even if data security could be considered part of Plaintiffs' "bargain" for medical services, the same fundamental flaw persists. An individual who bargains for data security and whose data is never accessed by third parties has received exactly what she paid for and not suffered a particularized injury, even if others suffered identity theft.

Therefore, the Court finds that the Group III Plaintiffs[21] have not alleged a concrete and particularized injury sufficient to establish their standing to bring their claims.

2. Causation

Defendants argue that all Plaintiffs have failed to adequately allege a causal connection between their alleged injuries and Defendants' conduct. More specifically, Defendants argue that the CCACs allege a "speculative chain" of events that belies a finding that their conduct is "fairly traceable" to Plaintiffs' injuries. See, e.g., Quest Mem. at 20-23; LabCorp. Mem. at 4-8. With one exception, the Court disagrees.

In addition to an injury-in-fact, Article III requires that Plaintiffs allege a "causal connection between" their injuries "and the conduct complained of." Lujan, 504 U.S. at 560-61. An alleged injury must be "fairly traceable" to Defendants' wrongful conduct and "not the result of the independent action of some third party not before the court." Id. (citation and alterations omitted). This requirement is "akin to 'but for' causation" and traceability can be found "even

[21] One Group III Plaintiff, minor child L.D., requires special consideration. Plaintiffs allege that L.D. provided CareCentrix with Personal Information; that L.D's mother, Andrea Hall, used a credit card to purchase services from CareCentrix; and that following the Data Breach, Hall experienced a fraudulent charge on her credit card. CareCentrix CCAC ¶¶ 30, 36. Critically, Hall does not assert any claims on her own behalf but sues solely on behalf of L.D. Id. ¶ 28. But Plaintiffs allege no facts suggesting that L.D.'s personal information was accessed or misused by any third party. Consequently, L.D. falls into Group III and lacks standing.

where the conduct in question might not have been a proximate cause of the harm, due to intervening events." Edmonson v. Lincoln Nat. Life Ins. Co., 725 F.3d 406, 418 (3d Cir. 2013). While a mere "speculative chain of possibilities" cannot establish traceability, Clapper, 568 U.S. at 414, even "an indirect causal relationship" can be sufficient to meet this standard. Hassan v. City of New York, 804 F.3d 295, 293 (3d Cir. 2015).

The Court agrees that one Sonic Plaintiff in Group II, D. Davis, has failed to plausibly allege a causal nexus between his injuries and Defendants' wrongful conduct. D. Davis alleges that he suffered identify theft on April 6, 2018, when an individual attempted to withdraw $1,700 from his bank account. Sonic CCAC ¶ 39. But Plaintiffs allege that the Data Breach begin four months later, in August 2018. Consequently, D. Davis' injuries cannot be traced to the Data Breach or Sonic's alleged conduct, and D. Davis lacks standing.[22]

On the other hand, the remaining Group I and II Plaintiffs have each alleged facts sufficient to satisfy the traceability requirement. The crux of Plaintiffs' theory of liability is that Defendants knew or should have known that AMCA's data security was insufficient, should not have provided AMCA with their Personal Information, and should have maintained better oversight over AMCA's data security practices. See, e.g., Quest CCAC ¶¶ 322-23, 325, 327, 421. As a result of these alleged acts and omissions, Plaintiffs were injured by the Data Breach. Simply put, Plaintiffs allege that they would not have had their Personal Information compromised by hackers "but for" Defendants' choice to contract with AMCA without maintaining any oversight. At this stage in

[22] Plaintiffs argue that dismissal of D. Davis' claims are premature because the "exact start date" of the Data Breach is uncertain. Pl. Opp. to Sonic Mem. at 13, ECF No. 168. The CCACs, however, expressly allege that the Data Breach occurred in a date range beginning in August 2018. Plaintiffs cannot now expand this range through a brief opposing a motion to dismiss.

the litigation, this is enough to allege that their injuries were caused by—and fairly traceable to—Defendants' conduct.[23]

Defendants argue that because third parties not before the Court contributed to the Plaintiffs' injuries—specifically, AMCA and criminal hackers—such injuries cannot be fairly traced to Defendants' conduct. But the participation of third parties does not defeat traceability where, as here, a plaintiff alleges facts suggesting a nonspeculative causal link. The CCACs allege facts detailing a clear series of events that resulted in the theft of Plaintiffs' Personal Information. While third parties may share in the fault, the indirect "but for" connection alleged by Plaintiffs is sufficient to allege traceability. See, e.g., Hassan, 804 F.3d at 293.

Additionally, Defendants contend that the complaints belie a finding of traceability because some Plaintiffs "severed the causal chain" with their own conduct when they provided some of their Personal Information directly to AMCA. LabCorp. Mem. at 4-5; see also Quest Mem. at 22. These arguments twist the facts and are contradicted by applicable law. The CCACs allege that Plaintiffs only provided additional information to AMCA after (and because) Defendants sent their Personal Information to AMCA in the first place. Again, Defendants cannot rely on the existence of contributing factors or intervening events to defeat Plaintiffs' standing. See, e.g., Edmonson, 725 F.3d at 418.

Defendants' remaining arguments regarding traceability are factual questions of causation that cannot be resolved on a motion to dismiss. For example, Defendants' argument that the

[23] Defendants assert that courts routinely dismiss data breach complaints on traceability grounds, but the cases they cite in support are misplaced. For example, in Anderson v. Kimpton Hotel & Rest. Grp., LLC, the plaintiffs failed to allege that the defendants took any insufficient or inadequate action with respect to the data breach. 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019). Not so here, as Plaintiffs allege that Defendants knew of AMCA's deficient cybersecurity and failed to act accordingly. Defendants also rely on In re Science Applications Int'l Corp. Backup Tape Data Theft Litig., where plaintiffs failed to allege that hackers obtained any information that could be used to cause the injuries they suffered. 45 F. Supp. 3d 14 (D.D.C. 2014). Again, not so here as Plaintiffs allege various personal information was compromised and misused.

specific information Plaintiffs provided was insufficient to allow criminals to commit identity theft is a question of fact more appropriately resolved on summary judgment or at trial. See, e.g., In re Marriott, 440 F. Supp. at 467 ("While Defendants may ultimately show, after the opportunity for discovery, that the alleged injuries are not caused by their data breach, it is premature to dismiss Plaintiffs' claims on grounds of traceability."). Plaintiffs here allege that the information taken was used to nefarious ends. See, e.g., LabCorp CCAC ¶¶ 16-18, 28-29. These allegations are sufficient at the pleading stage to establish causation. See In re SuperValu, Inc., 870 F.3d 763, 772 (8th Cir. 2017) ("At this stage of the litigation, we presume that these general allegations embrace those specific facts that are necessary to support a link between Holmes' fraudulent charge and the data breaches.") (citation and alterations omitted).

* * *

In sum, the Court finds that the Group III Plaintiffs have failed to establish their standing because they have failed to allege an injury-in-fact. Their claims are dismissed for lack of subject-matter jurisdiction. All Group I and II Plaintiffs except D. Davis have adequately alleged an injury-in-fact that is fairly traceable to Defendants' conduct. The Court therefore proceeds to Defendants' argument that Plaintiffs have failed to state a claim upon which relief may be granted.[24]

B. Choice of Law

Before delving into the merits of each surviving claim asserted by the CCACs, the Court must address Defendants' request to perform a choice of law analysis. Defendants urge the Court to apply the law of each Plaintiff's home state to their respective claims. Plaintiffs posture about

[24] The Court's determination that D. Davis and the Group III Plaintiffs lack standing disposes of each claim asserted in the CareCentrix and Inform CCACs. The Court therefore grants the CareCentrix and Inform Motions in their entirety.

what laws should apply—generally advocating that the laws of Defendants' home states apply to their nationwide, common law claims—but argue that any ruling on choice of law is premature at this juncture because Defendants have not engaged in a fulsome choice of law analysis. The Court agrees with Plaintiffs.

"[C]hoice of law analysis has routinely been found to be premature at the motion to dismiss phase of a class action lawsuit," because a choice of law analysis is fact-intensive and requires an inquiry on a claim-by-claim basis. In re Liquid Aluminum Sulfate Antitrust Litig., No. 16-2687, 2017 WL 3131977, at *16 (D.N.J. July 20, 2017) (declining to perform choice of law analysis at motion to dismiss phase because the defendants did not explain how any of the plaintiffs' common law claims conflict with the laws of the home state); Bang v. BMW of N. Am., LLC, No. 15-6945, 2016 WL 7042071, at *5 (D.N.J. Dec. 1, 2016) (declining to perform choice of law analysis at motion to dismiss phase because the case involved multiple defendants with multiple claims).[25] In the few cases where courts have addressed choice of law at the motion to dismiss phase, the issue was fully briefed by the parties. See Skeen v. BMW of N. Am., LLC, No. 13-1531, 2014 WL 283628, at *3-4 (D.N.J. Jan. 24, 2014); see also Cooper v. Samsung Elecs. Am., Inc., 374 F. App'x 250, 255 (3d Cir. 2010) (performing choice of law analysis at motion to dismiss phase when it required the court to analyze one plaintiff and one claim). Therefore, in contrast to the instant case, there was not a need for more fulsome development.

---

[25] The Court notes that in these cases, the choice of law analysis was arguably less complicated than the choice of law analysis here. There, the parties agreed that New Jersey's choice of law rules applied in deciding which states' laws applied. See In re Liquid Aluminum Sulfare Antitrust Litig., 2017 WL 3131977, at *16; Bang, 2016 WL 7042071, at *5 n.5. Here, on the other hand, the parties do not even agree about which states' choice of law rules apply, because cases transferred into an MDL have unique rules concerning choice of law. See In re Ford Motor Co. Ignition Switch Prods. Liability Litig., 174 F.R.D. 332, 348 (D.N.J. 1997).

Here, it is premature to decide choice of law issues at this stage. Defendants argue that sixteen different states' choice of law rules apply to Plaintiffs' common law claims,[26] but then state in a conclusory fashion that the result of the sixteen different states' choice of law analyses is that the laws of Plaintiffs' home states must govern Plaintiffs' claims. See Quest Mem. at 24, LabCorp Mem. at 14. Defendants do provide a few examples of what a choice of law analysis looks like in a few of Plaintiffs' home states, but not in each at-issue state. See Quest Mem. at 24-25; LabCorp Mem. at 15-16 & n.11. Similarly, Defendants provide examples of conflicts that exist between different states' laws, but pointing out the mere existence of conflicts does not itself allow the Court to perform the requisite claim-by-claim analysis. See Quest Mem. at 24 n.21; LabCorp Mem. at 14 n.10 (identifying differences in the different states' negligence and consumer protection laws but not, for example, in contract law or unjust enrichment).

The Court therefore concludes that because choice of law has not been fully briefed by the parties, further development on this point is warranted. See Bang, 2016 WL 7042071, at *5 n.5 ("Assuming that a conflict exists here between the laws of different states, the appropriate analysis on a motion to dismiss would be to examine which jurisdiction's laws apply to each of the Named Plaintiffs. No such analysis was undertaken by Defendant here."). That said, the Court may still address several arguments raised by Defendants in the Motions regarding Plaintiffs' common law claims, where the potentially-applicable states' laws are not meaningfully distinct. Moreover, Plaintiffs concede that the law of each Plaintiff's home state applies to their statutory claims. Pl. Opp. to Quest Mot. at 17 n.4. The Court thus proceeds to the merits of Plaintiffs' claims.

---

[26] Plaintiffs do not appear to dispute this initial argument.

C. Common Law Claims

The CCACs assert four common law claims against each Defendant on behalf of putative nationwide classes: (1) negligence; (2) negligence per se; (3) unjust enrichment; and (4) breach of implied contract. Defendants argue that each claim fails to state a claim upon which relief can be granted. The Court agrees as to Plaintiffs' claims for unjust enrichment and breach of contract but will permit their negligence and negligence per se claims to proceed.

1. Negligence

Plaintiffs have stated a claim for negligence under any potentially applicable state law. As Defendants recognize, the basic elements of negligence are the same in every state: duty, breach, causation, and damages. See, e.g., LabCorp Mem. at App. A. Plaintiffs have sufficiently pled each of these elements.

a. Duty

Defendants argue that they did not owe any duty to Plaintiffs with regards to their Personal Information. However, this is simply untrue. It is axiomatic that a defendant has a duty to protect a plaintiff against foreseeable harm. See, e.g., Saponaro v. Grindr LLC, 93 F. Supp. 3d 319, 326 (D.N.J. 2015) ("To determine whether a defendant owes a duty to the plaintiff, a 'significant consideration' is whether the plaintiff is a foreseeable victim of the defendant's conduct."). Here, Plaintiffs allege that "Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons." Quest CCAC ¶ 415; LabCorp CCAC ¶ 151; Sonic CCAC ¶ 177. The Court agrees. Once Defendants collected Plaintiffs' information, they

had a duty to protect Plaintiffs from foreseeable harm by taking reasonable precautions to safeguard that information.

Courts that have considered this argument in similar data breach cases have reached the same conclusion. For example, in In re Equifax, Inc. Customer Security Breach Litigation ("In re Equifax"), the court held that defendants had a duty to safeguard plaintiffs' personal information, flowing from the notion that "under traditional negligence principles, the Defendants owed a legal duty to the Plaintiffs to take reasonable precautions due to the reasonably foreseeable risk of danger of a data breach incident." 362 F. Supp. 3d 1295, 1321-27 (N.D. Ga. 2019). The Court in Brush v. Miami Beach Healthcare Group Ltd. similarly held that healthcare providers had a duty to safeguard their patients' personal information, explaining that "[i]t is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information." 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017).[27]

Defendants argue that notwithstanding In re Equifax and Brush, there is no "common law basis that Defendants had a duty to ensure that a third-party hacker would be unable to invade a database that is in the possession of a third-party vendor." Sonic Mem. at 23, ECF No. 147.3. This defines Defendants' duty to Plaintiffs far too narrowly. The duty to Plaintiffs arose when Defendants collected Plaintiffs' Personal Information and not, as Defendants try to frame the issue, when the Personal Information was stolen from AMCA by the hackers. Defendants owed Plaintiffs a duty of care to protect their Personal Information from foreseeable risks by taking

[27] Optum360 provides a string cite of states which it contends have explicitly rejected the notion that a defendant has a duty to safeguard a plaintiff's personal information. Optum360 MTD at 12 n.7. None of the cited cases are at all relevant or applicable. See, e.g., In re Anthem Data Breach Litig., 162 F. Supp. 3d 953, 975-78 (N.D. Cal. 2016) (applying Indiana law—which is not at issue in this case—to determine whether the state created a private right of action to bring a tort claim for failure to protect personal information); In re SuperValu Customer Data Sec. Breach Litig., No. 14-2586, 2018 WL 1189327, at *14 (D. Minn. Mar. 7, 2018) (dismissing plaintiff's negligence claim for failure to allege a cognizable injury and under the economic loss doctrine). Defendants attempts to refute this very simple truth of common law negligence—that one always owes another a duty to protect them from foreseeable harm—are unavailing.

reasonable precautions once they collected Plaintiffs information. That duty did not vanish when Defendants chose to contract with AMCA.

For similar reasons, Defendants likewise miss the mark by arguing that Defendants did not have a duty to oversee the operations of AMCA, an independent contractor. See, e.g., Quest Mem. at 26. The Court agrees that Defendants were not required to oversee all of AMCA's operations, but this does not absolve Defendants of their duty to take reasonable care by, for example, reasonably ensuring that the third-party collection agency they contracted with had adequate data security.

b. Breach

Plaintiffs allege that Defendants breached their duty to take reasonable efforts to safeguard Plaintiffs' Personal Information by, among other things, providing information to AMCA when they "knew or should have known that AMCA's web payments page was vulnerable to unauthorized access by third parties," and failing to implement measures to monitor, audit, or evaluate AMCA's data security practices. E.g., Quest CCAC ¶¶ 413, 423. Plaintiffs also plead specific facts bearing on Defendants' alleged lack of oversight, including that (a) an investigation would have revealed that AMCA's security practices failed to comply with several specific industry standards, see, e.g., Quest CCAC ¶¶ 330-332, and (b) Defendants did not learn of the Data Breach until two months after AMCA learned of it, see, e.g., id. ¶ 333.

While the existence of a duty is a question of law, the issue of whether a defendant's conduct breached that duty is typically reserved for the factfinder. See, e.g., Morris v. Krauszer's Food Stores, Inc., 300 N.J. Super. 529, 534 (N.J. App. Div. 1997). Consequently, the above allegations plead a breach of duty sufficient to survive the instant Motions. A factual determination

of whether Defendants' actions violated their duty to reasonably safeguard Plaintiffs' Personal Information is premature.

c. Causation

Plaintiffs allege that their "Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties." See e.g., Quest CCAC ¶ 424. More specifically, Plaintiffs maintain that "Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Information." E.g., Quest CCAC ¶ 425. Defendants reason that because none of Defendants' own databases were impacted by the alleged breach (only AMCA's), proximate causation does not exist. See, e.g., Sonic Mem. at 38 (quoting Allegheny Gen. Hosp. v. Philip Morris, Inc., 228 F.3d 429, 445 (3d Cir. 2000), for the theory that proximate causation does not exist where "an injury is indirect, remote, and many steps away from the alleged cause"). The Court disagrees.

Like breach of duty, causation is ordinarily a question of fact to be decided by the jury. See, e.g., In re Equifax, 362 F. Supp. 3d at 1319. Regardless, Defendants urge the Court to take a far too narrow approach to the issue of proximate causation. "Proximate cause is a cause which in the natural and continuous sequence, unbroken by an efficient intervening cause, produces the result complained of and without which the result would not have occurred." Broach-Butts v. Therapeutic Alts., Inc., 456 N.J. Super. 25, 40 (App. Div. 2018). Here, Plaintiffs allege that if Defendants had used reasonable care in selecting and monitoring their collection agency, AMCA would not have had access to Plaintiffs' Personal Information and the information would not have

been wrongfully accessed. For the purposes of a motion to dismiss, this chain of events is sufficient to satisfy proximate causation.[28]

d. Damages

For the reasons explained in the Court's standing analysis, supra Section IV.A.1, Plaintiffs have adequately alleged an injury as to the Groups I and II Plaintiffs. Each of the Plaintiffs in Groups I and II adequately alleged that the hackers accessed their Personal Information, which has resulted in either tangible or intangible harm. These allegations are sufficient to satisfy the damages prong of Plaintiffs' negligence claim at this stage.[29]

e. Group Pleading Against Sonic

Finally, Sonic argues that the Sonic CCAC impermissibly groups together Sonic USA and the Sonic Subsidiaries without pleading facts sufficient to impose individual liability on each defendant. The Court agrees.

Although Federal Rule of Civil Procedure 8(a) "does not require that a complaint contain detailed factual allegations," Plaintiffs must plead facts sufficient to "place Defendants on notice of the claims against each of them." Forero v. APM Terminals, No. 18-13754, 2019 WL 6168031,

---

[28] Despite Optum360's insistence to the contrary, the negligence analysis is no different as to Optum360. Although it is true that Quest already had a working relationship with AMCA prior to Quest and Optum360's partnership, the Quest CCAC alleges that Optum360 provided Quest patients' Personal Information to AMCA for collection. Quest CCAC ¶¶ 306-07. For this reason, Plaintiffs sufficiently allege that Optum360 likewise failed to reasonably secure Personal Information in its possession and was a significant actor in the chain of events that led to the theft of Plaintiffs' information.

[29] Defendants argue that the economic loss rule, which governs many of the at-issue state laws, bars Plaintiffs' negligence claim based upon economic injury alone. The Court is satisfied that the economic loss doctrine under many, if not all, of the potentially-applicable states' laws would not bar Plaintiffs claims because Plaintiffs were an "identifiable class that the defendant should have reasonable foreseen was likely to be injured by the defendant's conduct." Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426 (5th Cir. 2013) (New Jersey law); see also, e.g., Marvin Lumber & Cedar Co. v. PPG Indus., Inc., 223 F.3d 873, 882 (8th Cir.) (Minnesota law). That said, because the Court declines to address choice of law issues at this juncture, Defendants can renew this argument following discovery. For the same reason, the Court defers consideration on Defendants' arguments that the laws of particular states do not recognize some of the intangible injuries claimed by the Group II Plaintiffs. See, e.g., Optum Mem. at 26-27, ECF No. 149.1; Quest Mem. at 35-37.

at *5 (D.N.J. Nov. 19, 2019) (quoting Sheeran v. Blyth Shipholding S.A., No. 14-5482, 2015 WL 9048979, at *3 (D.N.J. Dec. 16, 2015)). "[T]o the extent [a plaintiff] seeks to lump several defendants together without setting forth what each particular defendant is alleged to have done, he has engaged in impermissibly vague group pleading." Ingris v. Borough of Caldwell, No. 14-855, 2015 WL 3613499, at *5 (D.N.J. June 9, 2015).

Only one Sonic Plaintiff—Anderson, a Group II Plaintiff—has demonstrated Article III standing. Anderson alleges that she was a "Sonic patient" who obtained services at "one or more of Sonic's laboratories" from 2015 to 2019, that she provided Personal Information to "Sonic's laboratories," and that "Sonic's laboratories" forwarded her information to AMCA. Sonic CCAC ¶¶ 21-23. As discussed above, Defendants had a common law duty to safeguard Personal Information that they collected and maintained, but Anderson has failed to allege which of the fourteen named Sonic entities possessed her information.[30]

Anderson alleges that she received notice of the Data Breach from two Sonic Subsidiaries: Clinical Pathology Laboratories, Inc. ("CPL") and Austin Pathology Associates ("Austin Pathology"). Sonic CCAC ¶¶ 25-26. But the mere fact that these entities provided such notice does not permit the Court to infer that Anderson visited these Sonic Subsidiaries and provided them with her Personal Information, or that CPL and/or Austin Pathology provided Anderson's Personal Information to AMCA. To sufficiently plead a duty of care, any amended pleading must expressly allege the specific entities that collected, maintained, and failed to protect Anderson's Personal Information. See Shaw v. Hous. Auth. of Camden, No. 11-4291, 2012 WL 3283402, at

[30] Manifestly, it is implausible that Anderson provided her information to every Sonic entity, as the entities are located all over the country. Sonic CCAC ¶ 51.

*2 (D.N.J. Aug. 10, 2012) ("Even under the most liberal notice pleading requirements of Rule 8(a), a plaintiff must differentiate between defendants.").

Similar issues plague Anderson's negligence claim against the parent, Sonic USA. Plaintiffs concede that they do not seek to pierce Sonic USA's corporate veil and instead wish to hold Sonic USA "liable for its own actions" with respect to its information security policies. Pl. Opp. to Sonic Mot. at 19-20. Again, however, the Sonic CCAC is devoid of any allegation that Sonic USA, as opposed to "one or more" of its subsidiaries, ever collected, maintained, or transmitted Anderson's Personal Information. Without such factual allegations, no duty of care arises.

Anderson's negligence claims against Sonic are therefore dismissed without prejudice.

2. Negligence Per Se

Plaintiffs allege that Defendants were negligent per se by violating the Health Insurance Portability and Accountability Act ("HIPAA") and Section 5 of the Federal Trade Commission Act ("Section 5"). Plaintiffs contend that Defendants violated these statutes by failing to secure their Personal Information. Defendants counter that Plaintiffs' negligence per se clams are not cognizable under the relevant states' law.

Where recognized, a theory of negligence per se permits a plaintiff to establish the traditional negligence elements of duty and breach by proving that a defendant violated a statutory standard of conduct. See, e.g., In re Marriott, 440 F. Supp. 3d at 478 (permitting negligence per se claim to proceed under Georgia law arising from alleged "failure to use reasonable measures to protect personal information," in violation of Section 5). But unlike Plaintiffs' standard negligence claims, the law governing negligence per se varies drastically between states. For example, of the sixteen potential state laws that may apply to the claims of Plaintiffs with Article III standing, four

states do not recognize independent claims for negligence per se,[31] and at least seven states do not recognize claims for negligence per se based on laws without private rights of action, like HIPAA and Section 5 of the FTC.[32]

Consequently, it is premature to assess the merits of Plaintiffs' negligence per se claims before determining the applicable state law. The Court therefore denies LabCorp's, Quest's, and Optum's motion to dismiss Plaintiffs' negligence per se claim without prejudice.[33] Defendants may renew their motion at the close of discovery.

3. Unjust Enrichment

The CCACs further allege that Defendants were unjustly enriched by their collection of and failure to secure Personal Information. See, e.g., Quest CCAC ¶¶ 445-46. Under any applicable state law, however, Plaintiffs' unjust enrichment claims fail because Plaintiffs allege no facts showing that Defendants have been enriched. See Pl. Opp. to Quest Mem. at 56-57 (acknowledging that a "benefit conferred" is an essential element of a claim for unjust enrichment).

Plaintiffs allege that Defendants "received a monetary benefit from Plaintiffs and Class Members conferring upon them [Plaintiffs'] Personal Information which Defendants retain and use for business purposes and profit." See, e.g., Quest Compl. ¶ 446. But beyond vague allegations

---

[31] See Cent. Okla. Pipeline, Inc. v. Hawk Field Servs., LLC, 400 S.W.3d 701, 712 (Ark. 2012) (Arkansas); Quiroz v. Seventh Ave. Ctr., 140 Cal. App. 4th 1256, 1284-85 (2006) (California); Bray v. Marriott Int'l, 158 F. Supp. 3d 441, 444-45 (D. Md. 2016) (Maryland); In re TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83, 91 n.4 (D. Mass. 2007) (Massachusetts).

[32] See Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1365 (S.D. Fla. 2015) (Florida); Coleman v. Danek Med., 43 F. Supp. 2d 629, 633 n.2 (S.D. Miss. 1998) (Mississippi); Abdale v. N. Shore-Long Island Jewish Health Sys., Inc., 19 N.Y.S.3d 850, 859 (N.Y. Sup. Ct. 2015) (New York); Hetzel v. JPMorgan Chase Bank, N.A., 2014 WL 7336863, at *7 (E.D.N.C. Dec. 22, 2014) (North Carolina); Sheldon v. Kettering Health Ntwork, 40 N.E.3d 661, 674 (Ohio Ct. App. 2015) (Ohio); Wagner v. Anzon, Inc., 684 A.2d 570, 575 (Pa. Super. 1996) (Pennsylvania); Faber v. Ciox Health, LLC, 944 F.3d 593, 599 n.5 (6th Cir. 2019) (Tennessee).

[33] Anderson's negligence per se claim against Sonic is dismissed without prejudice for the same reasons discussed above, i.e., that Anderson has failed to allege facts showing which Sonic entities failed to reasonably safeguard her Personal Information.

that Defendants collected information for "commercial gain," id. ¶ 412, the CCACs contain no facts showing how Defendants reaped monetary benefits or otherwise profited from Plaintiffs' Personal Information. See Pirozzi v. Apple Inc., 913 F. Supp. 2d 840, 852 (N.D. Cal. 2012) (dismissing unjust enrichment claim for failure to allege how defendant was benefited by data collection); cf. In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 970 (S.D. Cal. 2014) ("In re Sony I") (finding no grounds for equitable restitution arising from data breach because defendant "did not benefit financially from the Data Breach").

Plaintiffs argue that courts have recognized that Personal Information is valuable to a business who retains it and uses it. Pl. Opp. to Quest Mot. at 57. This is certainly true in situations where businesses commoditize or receive an independent pecuniary benefit from holding the Personal Information. For example, in In re Yahoo! Inc. Customer Security Data Breach Litigation, the court held that the plaintiffs' personal information was valuable to the defendant because plaintiffs alleged that defendant used the information for targeted advertising. No. 16-2752, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) ("In re Yahoo!"). Similarly, in In re Marriott, the court held that the plaintiffs' personal information was valuable to the defendant because plaintiffs alleged that the defendant collected the information to better target customers and increase profits. 440 F. Supp. 3d at 461. Here, on the other hand, there is no such allegation that Defendants, companies that provided medical diagnostic services for Plaintiffs, receive any additional value from Plaintiffs Personal Information.[34] For this reason, Plaintiffs have failed to state a claim for unjust enrichment.

[34] Plaintiffs allege that Defendants used their Personal Information to ensure payment for their health care services from patients directly or their insurers. See, e.g., Quest CCAC ¶¶ 304-09. This is not an independent benefit that Defendants received: Plaintiffs were required to make these payments as a result of the services rendered by Defendants (blood work). Plaintiffs have failed to allege that Defendants received an independent benefit from their Personal Information.

4. Breach of Implied Contract

Next, Plaintiffs allege that when they provided their Personal Information, Defendants agreed to implied contracts to secure their Personal Information and provide timely notice of any data breach.[35] Quest CCAC ¶ 461. Defendants argue that the mere fact that Plaintiffs provided Personal Information does not suggest that Defendants agreed to guarantee the safety of that information, at least not without accompanying factual allegations to show mutual assent to those terms. The Court agrees.

Mutual assent is an essential element of an implied contract claim under any applicable state law, as Plaintiffs acknowledge. See Pl. Opp. to Quest Mot. at 32. In similar situations, courts have consistently held that the fact that a defendant required plaintiffs to provide personal information does not alone support the inference that the parties agreed for the defendant to secure this information. For example, in Brush, the plaintiff was required to provide Personal Information when checking into the defendants' healthcare facility to obtain medical treatment. 238 F. Supp. 3d at 1369. The plaintiff asserted "that based on her dealings with the Defendants, an agreement to protect her private information can be implied" and that "Defendants knew she expected them to protect her data." Id. at 1368. The court disagreed with the plaintiff, holding that such dealings did not create an implied contract:

> Nothing in the Plaintiff's Complaint gives rise to a factual inference that the Defendants tacitly agreed to secure her personal data in exchange for remuneration. It is clear from the Plaintiff's allegations that she transacted to receive healthcare services from the Defendants—not data security services beyond the privacy requirements already imposed on the Defendants by federal law. Accordingly, the Court cannot imply a contract to provide data security services based on the conduct of the parties.

[35] Plaintiffs have withdrawn their implied contract claim against Optum360. Pl. Opp. to Quest Mot. at 31 n.8.

Id. at 1369.

Similarly, in Longnecker-Wells v. Benecard Services Inc., plaintiff-employees claimed that the defendant-employer breached an implied contract by failing to adequately safeguard the plaintiffs' information, which the employer held as a condition of employment. 658 F. App'x 659, 662 (3d Cir. 2016). The Third Circuit concluded that this allegation was not sufficient to infer mutual assent:

> Plaintiffs have failed to plead any facts supporting their contention that an implied contract arose between the parties other than that [Defendant] required Plaintiffs' personal information as a prerequisite to employment. This requirement alone did not create a contractual promise to safeguard that information, especially from third party hackers.

Id.[36] By the same token, here Plaintiffs paid Defendants to perform healthcare services, i.e., blood work. Incidentally, Plaintiffs were required to provide Defendants with their personal information to ensure Defendants received payment from Plaintiffs or their insurers. Plaintiffs do not credibly allege that Defendants assented to safeguard Plaintiffs' Personal Information to an extent beyond what is already required by federal law.

Plaintiffs rely on several cases that allowed similar breach of implied contract claims to proceed at a motion to dismiss stage. See Rudolph v. Hudson's Bay Co., No. 18-8472, 2019 WL 2023713, at *10-11 (S.D.N.Y. May 7, 2019); In re Marriott, 440 F. Supp. 3d at 485-86; Castillo v. Seagate Tech., LLC, No. 16-1958, 2016 WL 9280242, at *8-9 (N.D. Cal. Sept.14, 2016). Critically, however, in each of these cases, plaintiffs pled that the defendants "through privacy

---

[36] See also Corona v. Sony Pictures Entm't Inc., No. 14-9600, 2015 WL 3916744, at *6 (C.D. Cal. June 15, 2015) ("Here, Plaintiff alleges that the parties entered into a contract of employment in exchange for compensation and other benefits. To receive compensation and other benefits, Plaintiffs were required to provide [defendant] their [personal information]. Plaintiffs adequately allege that [defendant] consciously and deliberately failed to maintain an adequate security system. However, there are no facts indicating that [defendant's] acts were intended to frustrate the agreed common purpose of the agreement, i.e., employment in exchange for compensation and benefits.") (citations omitted).

policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard" the plaintiffs' Personal Information. Longenecker-Wells, 685 F. App'x at 663 (citation and quotation marks omitted). Plaintiffs fail to adequately plead these additional facts.

Plaintiffs come closest to identifying a policy or practice from which the Court could infer an implied contract by pointing to statements on Defendants' websites, which Plaintiffs claim indicate that Defendants committed to protect patient information. See Quest CCAC ¶¶ 340-47; LabCorp CCAC ¶¶ 87-93; Sonic CCAC ¶¶ 69-74, 102-08. However, each identified statement indicates, at most, that Defendants intended to abide by the privacy requirements outlined in HIPAA. See, e.g., Quest CCAC ¶ 346 ("The requirements—which stem from contractual duties as well as duties under [HIPAA]—were violated. Defendants failed to maintain the privacy and security [of] patients [protected health information], and failed to inform patients that their Personal Information was disclosed."); LabCorp CCAC ¶ 89 ("In this HIPAA-mandated privacy notice, LabCorp agrees that it will keep [protected health information] of its patients, including Plaintiffs and Class Members, confidential and protected from unauthorized disclosure."); Sonic CCAC ¶ 73 ("Sonic is well aware of HIPAA's requirements regarding patient privacy and has adopted a Notice of Privacy Practices for Protected Health Information."). Statements of Defendants' intent to follow federal law do not support an independent cause of action for breach of implied contract. See Brush, 238 F. Supp. 3d at 1369.[37]

More importantly, the same privacy notices cited by Plaintiffs also explicitly state that Defendants did not ensure the privacy and safety of Plaintiffs' information. See Quest CCAC ¶ 347 ("As a result, while we strive to protect your personal information, we cannot ensure or

[37] Moreover, only three Plaintiffs with standing, Vieyra, Hollway, and Benadom, allege that they "reviewed and agreed to" any of the Defendants' policies before obtaining services. Quest CCAC ¶¶ 24, 46, 149. The remaining Plaintiffs could not have plausibly assented to an implied contract based on policies they had never read.

warrant the security of any information you transmit to us or receive from us."); Website Privacy Policy, LabCorp, https://www.labcorp.com/hipaa-privacy/web-privacy-policy (last visited Dec. 16, 2021) ("Please be aware that while We take appropriate steps to safeguard the security of Your Personal Information, the transmission of information over the Internet is not completely secure and therefore You do this at Your own risk. Once We receive Your Personal Information We will implement strict security procedures with the objective of preventing unauthorized access.") (cited at LabCorp CCAC ¶ 91 n.40). These statements make doubly clear that Defendants did not implicitly assent to a contract to protect Plaintiffs' Personal Information.

In sum, Plaintiffs do not, and cannot, allege that Defendants made any implicit promise to protect Personal Information from third-party hackers or provide notice of a data breach beyond its obligations under applicable law. Plaintiffs' breach of implied contract claim is dismissed for failure to allege mutual assent.

D. Consumer Protection Statutes

Plaintiffs collectively assert 22 statutory consumer protection claims under the laws of 19 states. Of these, nine claims are brought solely on behalf of Group III Plaintiffs without Article III standing and thus, need not be considered.[38] Plaintiffs have also withdrawn their consumer protection claims under two Ohio statutes. See Pl. Opp. to Quest Mot. at 40; Pl. Opp. to LabCorp

[38] Plaintiffs' consumer protection claims under the following states' law fall under this category: (1) Connecticut (all CareCentrix Plaintiffs), CareCentrix CCAC ¶¶ 187-203; (2) Indiana (Quest Plaintiff Walden), Quest CCAC ¶¶ 80, 558-80; (3) Iowa (Quest Plaintiff Dirks), id. ¶¶ 94, 592-602; (4) Kansas (Quest Plaintiff A. Finch and LabCorp Plaintiff D. Finch), id. ¶¶ 104, 611-26; LabCorp CCAC ¶¶ 22, 284-99; (5) Kentucky (Quest Plaintiffs Green and Perry and LabCorp Plaintiff Rothwell), Quest CCAC ¶¶ 118, 127, 635-45; LabCorp CCAC ¶¶ 23, 308-18; (6) Maryland (LabCorp Plaintiffs Jerry and Kaplan), LabCorp CCAC ¶¶ 24-25, 319-32; (7) Missouri (Quest Plaintiff Rikard), Quest CCAC ¶¶ 165, 665-73; (8) New Hampshire (Quest Plaintiff Jaworowski), id. ¶¶ 174, 682-90; and (9) Oklahoma (LabCorp Plaintiff William-Winters and Sonic Plaintiff Collinsworth), LabCorp CCAC ¶¶ 38, 410-421; Sonic CCAC ¶¶ 11, 241-53.

Mot. at 29 n.18. Consequently, 11 consumer protection claims under the laws of nine states remain for consideration.[39]

Before analyzing each individual cause of action, the Court highlights some general principles. Initially, most consumer protection claims require a plaintiff to plead the same general elements: (1) conduct prohibited by the statute; (2) an injury; and (3) causation between the prohibited conduct and the injury.[40] Still, the conduct and injury necessary to plead a valid claim vary significantly from statute to statute, and some statutes impose additional requirements, such as reliance. With respect to prohibited conduct, the statutes generally proscribe fraudulent conduct, i.e., misrepresentations and knowing material omissions, and "deceptive" conduct, which encompasses practices beyond common law fraud but must still have some capacity to mislead a consumer. Some statutes also prohibit "unfair" practices, a nebulous concept which encompasses a still broader range of commercial conduct. Defendants effectively challenge the sufficiency of the CCACs as to all elements of each remaining consumer protection claim.

[39] At least one claim brought under the following statutes survives the Court's Article III standing analysis: (1) the California Consumers Legal Remedies Act, Cal. Civ. Code § 1770 ("CLRA"); (2) the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 ("UCL"); (3) the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1) ("FDUTPA"); (4) the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. ch. 93A, § 2 ("MACPA"); (5) the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.903 ("MICPA"); (6) the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1 ("MNCFA"); (7) the Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. Ann. § 325D.44, subd. 1(13) ("MNUTPA"); (8) the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2 ("NJCFA"); (9) Section 349 of the New York General Business Law ("NYGBL"); (10) the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1(a) ("NCUDTPA"); and (11) the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. Ann. § 201-2 ("PUTPCPL").

[40] See Steroid Hormone Prod. Cases, 104 Cal. Rptr. 3d 329, 337 (Cal. 2010) (CLRA); Rollins, Inc. v. Butland, 951 So.2d 860, 869 (Fla. Dist. Ct. App. 2006) (FDUTPA); Hanrahran v. Specialized Loan Servicing, LLC, 54 F. Supp. 3d 149, 153-54 (D. Mass. 2014) (Mass. CPA); Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 781-82 (W.D. Mich. 2006) (Mich. CPA); Johannessohn v. Polaris Indus., Inc., 450 F. Supp. 3d 931, 951 (D. Minn. 2020) (Minn. CFA); Int'l Union of Operating Engineers Loc. No. 68 Welfare Fund v. Merck & Co., 192 N.J. 372, 389 (2007) (NJCFA); Goldemberg v. Johnson & Johnson Consumer Companies, Inc., 8 F. Supp. 3d 467, 478 (S.D.N.Y. 2014) (NYGBL); Gilbane Bldg. Co. v. Fed. Rsrv. Bank of Richmond, Charlotte Branch, 80 F.3d 895, 902 (4th Cir. 1996) (NCUDTPA); Yocca v. Pittsburgh Steelers Sports, Inc., 854 A.2d 425, 438 (Pa. 2004) (PUTPCPL). The UCL and MNUTPA operate differently and are discussed below.

The Parties also dispute the extent to which the heightened pleading requirements of Federal Rule of Civil Procedure 9(b) apply to Plaintiffs' claims. Rule 9(b) applies to claims that "sound in fraud." In re Suprema Specialties, Inc. Sec. Litig., 438 F.3d 256, 269 (3d Cir. 2006). Thus, Rule 9(b) applies to a consumer protection claim only to the extent it asserts fraudulent conduct by the defendant. For example, in Katz v. Ambit Ne., LLC, No. 20-1289, 2021 WL 2680184, at *7 (D.N.J. June 29, 2021), the court concluded that Rule 9(b) applied to an NJCFA claim to the extent it relied on a misrepresentation or knowing omission, but not to the extent defendant allegedly violated the NJCFA's general prohibition of "unconscionable market practices."[41] Consequently, Plaintiffs must satisfy Rule 9(b) to the extent their statutory claims rely on alleged misrepresentations and knowing omissions made by Defendants, while Rule 8 applies to the extent Plaintiffs allege other deceptive or unfair conduct.

The CCACs set forth two broad theories of liability under each consumer protection statute. First, Plaintiffs allege that Defendants made misrepresentations and knowing omissions related to their data security practices. In this respect, they allege that had they "known that [Defendants] would fail to protect" their respective Personal Information, they would not have used Defendants for medical services and their Personal Information would not have been stolen. See, e.g., Quest CCAC ¶¶ 31, 69, 163. Beyond these misrepresentations and omissions, Plaintiffs allege no other "deceptive" conduct that they claim led to their purchase of services from Defendants. Second,

[41] Courts that have considered some of the other remaining statutes at issue are in accord that while a fraud-based consumer protection claim must be particularly pled, claims arising from some other actionable conduct need only satisfy the more forgiving "plausibility" standard of Rule 8. See, e.g., Morano v. BMW of N. Am., LLC, 928 F. Supp. 2d 826, 833 (D.N.J. 2013) ("[A]t least as to a fraud-based FDUTPA claim, the heightened pleading standard of Rule 9(b) should apply."); Kearns v. Ford Motor Co., 567 F.3d 1120, 1125 (9th Cir. 2009) (reaching same conclusion under CLRA & UCL) In re Gen. Motors LLC Ignition Switch Litig., 257 F. Supp. 3d 372, 421 (S.D.N.Y. 2017) (same under Mich. CPA); In re Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d 514, 540-41 (M.D. Pa. 2021) ("While plaintiffs who allege fraudulent practices under the UTPCPL must meet Rule 9(b)'s particularity standard, complaints that rely on the statute's prohibition of "deceptive" business practices need not."). The NYGBL appears to be an outlier. Courts have held that even omission and misrepresentation-based claims under the NYGBL need not be pled with particularity. See, e.g., Oden v. Bos. Sci. Corp., 330 F. Supp. 3d 877, 902 (E.D.N.Y. 2018).

Plaintiffs separately allege that Defendants' failure to maintain adequate cybersecurity procedures or oversee AMCA's cybersecurity procedures was an "unfair" or abusive practice that led to the Data Breach and, in turn, their injuries. See, e.g., Quest CCAC ¶¶ 523, 553(a)-(c).

Generally, the misrepresentation and knowing omission-based claims brought under Plaintiffs' first theory are governed by the particularity requirements of Rule 9(b) because the allegations sound in fraud. See, e.g., Katz, 2021 WL 2680184, at *7.[42] On the other hand, Rule 8(a) generally applies to claims brought under the second theory of liability.

With these principles in mind, the Court proceeds to analyze Plaintiffs' individual statutory claims.

1. New Jersey Consumer Fraud Act & North Carolina Unfair and Deceptive Trade Practices Act

New Jersey resident Jairam asserts claims against Quest and Optum360 under the NJCFA, while North Carolina residents Vazquez and Wrenn assert claims against LabCorp under the NCUDTPA. In addition to disputing the merits of Plaintiffs' claims, Quest, Optum360, and LabCorp each contend that they are exempt from these statutes as "learned professionals." The Court agrees that Quest and LabCorp are exempt and further concludes that Jairam has failed to state an NJCFA claim against Optum360.[43]

[42] With respect to alleged misrepresentations, Rule 9(b) requires a plaintiff to plead "all of the essential factual background that would accompany the first paragraph of any newspaper story—that is, the 'who, what, when, where and how' of the events at issue." In re Suprema Specialties, Inc. Sec. Litig., 438 F.3d at 276-77 (citation and quotation marks omitted). This standard is slightly relaxed for knowing omissions, but still more stringent than Rule 8. "Because a plaintiff alleging an omission-based fraud will not be able to specify the time, place, and specific content of an omission as would a plaintiff in a false representation claim, allegations of a fraudulent omission are not held to the same standard of specificity." Kennedy v. Samsung Elecs. Am., Inc., No. 14-4987, 2015 WL 2093938, at *3-4 (D.N.J. May 5, 2015) (citation and quotation marks omitted). But the complaint must still be "sufficiently specific to enable [the defendant] to prepare a responsive pleading." Id.

[43] While the Quest CCAC ostensibly brings NJCFA claims against Quest on behalf of every Quest Plaintiff, see Quest CCAC ¶¶ 466-75, the Court deems all such claims except Jairam's withdrawn in light of Plaintiffs' concession that "Plaintiffs' home state law" applies to each statutory claim. Pl. Opp. to Quest Mot. at 17 n.4. The LabCorp CCAC likewise asserts NCUDTPA claims against LabCorp on behalf of each LabCorp Plaintiff, see LabCorp ¶¶ 202-10, and Plaintiffs make no similar concession regarding choice of law in response to LabCorp's Motion. Regardless, the

a. The Learned Professional Exemption

The NJCFA and NCUDTPA each exempt "learned professionals"—i.e., individuals practicing in certain professions—from consumer fraud claims arising from transactions in their professional capacity. See N.C. Gen. Stat. § 75-1.1(b) ("[C]ommerce . . . does not include professional services rendered by a member of a learned profession."); Macedo v. Dello Russo, 178 N.J. 340, 345-46 (2004) ("[L]earned professionals [are] beyond the reach of the [NJCFA] so long as they are operating in their professional capacities."). "The rationale underlying the learned professionals exception is that uniform regulation of an occupation, where such regulation exists, could conflict with regulation under [consumer fraud statutes]." Lee v. First Union Nat. Bank, 199 N.J. 251, 264 (2009).

Medical diagnostic providers qualify as "learned professionals" eligible for the exemption. See Leslie v. Quest Diagnostics, Inc., No. 17-1590, 2019 WL 4668140, at *4 (D.N.J. Sept. 25, 2019) ("Quest . . . qualifies as a learned professional covered by other state regulation rendering a claim under the New Jersey or North Carolina consumer protection statutes incognizable."); see also Sykes v. Health Network Sols., Inc., 828 S.E.2d 467, 472 (N.C. 2019) (NCUDTPA exception applies to entities). Moreover, the exception extends to matters "affecting" professional services. Sykes, 828 S.E.2d at 472 (NCUDTPA exception applied to defendants' anonymous complaint to medical board because making the complaint was "integral to their role in ensuring the provision of adequate medical care"); Macedo v. Dello Russo, 178 N.J. 340, 345-46 (2004) (advertising for professional services exempt from NJCFA); DiCarlo v. St. Mary Hosp., 530 F.3d 255, 268 (3d Cir. 2008) (billing practices for professional services exempt from NJCFA).[44]

---

potential inclusion of out-of-state plaintiffs does not alter the Court's conclusion that LabCorp is exempt from the NCUDTPA.

[44] Defendants also argue that Pennsylvania recognizes a learned professional exception to the PUTPCPL, relying on Foflygen v. R. Zemel, M.D. (PC), 615 A.2d 1345, 1354-55 (Penn. 1992). The alleged deceptive practices in Foflygen

Plaintiffs do not dispute that Quest and LabCorp are "learned professionals" but contend that their allegations concern conduct outside Defendants' professional capacity. In support, Plaintiffs rely on (1) a New Jersey Supreme Court opinion that expressed "serious doubts" as to whether billing and collection provisions in a nursing home agreement fell within the exception, while declining to reach the issue, Manahawkin Convalescent v. O'Neill, 217 N.J. 99, 124 (2014); and (2) a dissent issued by a judge of the North Carolina Court of Appeals, opining that the exception is limited to the performance of work "[c]onforming to the standards of a profession." Phillips v. A Triangle Women's Health Clinic, Inc., 573 S.E.2d 600, 605 (N.C. 2002) (Green, J. dissenting). The Court is unpersuaded.

Plaintiffs' allegations principally relate to Defendants' duty to maintain the confidentiality of their patients' financial information, which is a regulated area of Defendants' profession under HIPAA. See 42 U.S.C § 1320d(4) (defining "health information" governed by HIPAA to include information that relates to "the past, present, or future payment for the provision of health care"). This places the instant action well within the rationale of the learned professional exception, as articulated by Lee and the Phillips dissent, and distinguishes the instant matter from the doubts expressed by the New Jersey Supreme Court in Manahawkin. Consequently, Plaintiffs' NJCFA and NCUPTA claims against LabCorp and Quest are barred and dismissed with prejudice.

On the other hand, Optum360 is not itself a learned professional and has cited no cases suggesting that New Jersey or North Carolina has extended the exception to contractors of learned professionals. The Court must therefore assess the merits of Jairam's NJCFA claim against Optum360.

---

concerned the effects of an actual medical procedure, as opposed to "related" practices. The Court need not determine whether Pennsylvania's exception extends to related practices in light of its determination, infra Section IV.D.8, that the Pennsylvania-based Plaintiffs have failed to allege reliance.

b. Jairam's NJCFA Claim Against Optum360

To plead a claim under the NJCFA, a Plaintiff must allege "(1) unlawful conduct;[45] (2) an ascertainable loss; and (3) a causal relationship between the defendants' unlawful conduct and the plaintiff's ascertainable loss." Int'l Union of Operating Engineers Loc. No. 68 Welfare Fund, 192 N.J. at 389. "The NJCFA creates three categories of unlawful practices: affirmative acts, knowing omissions, and violations of state regulations."[46] Arcand v. Brother Int'l Corp., 673 F. Supp. 2d 282, 296 (D.N.J. 2009). In all cases, the unlawful conduct must be (a) "in connection" with the sale or advertisement of a product or service, id. at 296-97, and (b) "misleading and . . . outside the norm of reasonable business practice in that it will victimize the average consumer," Katz, 2021 WL 2680184, at *8. With respect to omissions, a plaintiff must further allege that the defendant "(1) knowingly concealed (2) a material fact (3) with the intention that the consumer rely upon the concealment." Arcand, 673 F. Supp. 2d at 297 (citing Judge v. Blackfin Yacht Corp., 357 N.J. Super. 418, 426 (App. Div. 2003)). There must also be a duty to disclose the omitted facts. Id.

Jairam has failed to sufficiently plead an unlawful practice perpetrated by Optum360. First, no affirmative misrepresentations related to data security are attributed to Optum360. While Plaintiffs refer to several policies and notices issued by Quest, see Quest CCAC ¶¶ 340-47, they allege no similar representations by Optum360.[47]

[45] The NJCFA prohibits "any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with [a] sale or advertisement." N.J.S.A. § 56:8-2.

[46] "Regulatory violations" in this context refers to regulations promulgated under the NJCFA (i.e., not to outside regulations). See Davis v. Bankers Life & Cas. Co., No. 15-3559, 2016 WL 7668452, at *9 (D.N.J. Dec. 23, 2016).

[47] For the same reason, Plaintiffs' remaining consumer protection claims against Optum360 fail to the extent they allege affirmative misrepresentations.

Second, Jairam has not adequately pled that Optum knowingly concealed a material fact that it had a duty to disclose. Plaintiffs cite no authority to suggest that a third-party contractor of a consumer-facing business has a duty to disclose material facts to the business's customers, particularly where the contractor made no related affirmative statements prior to the subject transaction. Certainly, there is no "general duty to disclose to the entire world." In re Equifax, 362 F. Supp. 3d at 1337. Indeed, Jairam does not allege she had any relationship, contact, or even awareness of Optum360 prior to her purchase of services from Quest, nor does she allege that Optum360 made any statements that would require a more fulsome disclosure to avoid misleading the consumer public.

Finally, Optum360's alleged failure to oversee AMCA's data security is not a separately viable "unconscionable practice" because such failure could not conceivably have had a "capacity to mislead" in connection with Jairam's purchase of services from Quest. See Katz, 2021 WL 2680184, at *8. The Court therefore dismisses Jairam's NJCFA claim against Optum360 for failure to plead an unlawful practice.[48]

2. Minnesota Consumer Fraud Act

Minnesota resident Hollway asserts claims against Quest and Optum360 under the MNCFA.[49] Hollway has plausibly alleged a MNCFA claim against Quest arising from Quest's alleged failure to disclose material facts related to its relationship with AMCA.

---

[48] The Court below addresses Jariam's separate claim that Optum360's allegedly inadequate notice of the Data Breach violated the New Jersey Customer Security Breach Disclosure Act, a statute privately enforceable through the NJCFA. See infra Section IV.E.4.

[49] The Quest CCAC asserts claims under the MNCFA and MNUDTPA on behalf of all Quest Plaintiffs against Optum360. Quest CCAC ¶¶ 476-94. As with their NJCFA claims, the Quest Plaintiffs have effectively withdrawn the claims of out-of-state plaintiffs by conceding that the law of each Plaintiffs' home state applies to statutory claims. Pl. Opp. to Quest Mot. at 17 n.4.

To plead a MNCFA claim, a plaintiff must allege that "the defendant engaged in conduct prohibited by the statute[50] and that the plaintiff was damaged thereby." Johannessohn, 450 F. Supp. 3d at 951 (citing Grp. Health Plan, Inc. v. Philip Morris Inc., 621 N.W.2d 2, 12 (Minn. 2001)). Both misrepresentations and knowing omissions are actionable under the MNCFA. Id. at 951-52. A plaintiff must also allege a "causal nexus between the plaintiff's injuries and the defendant's wrongful conduct," though a plaintiff need not have relied upon such wrongful conduct. Cleveland v. Whirlpool Corp., No. 20-1906, 2021 WL 3173702, at *8 (D. Minn. July 27, 2021) (citing Wiegand v. Walser Auto. Grps., Inc., 683 N.W.2d 807, 811 (Minn. 2004)). Finally, a private plaintiff must allege the existence of a "public benefit" in bringing the suit. See Ly v. Nystrom, 615 N.W.2d 302, 314 (Minn. 2000).

Hollway asserts both misrepresentation and omission-based claims against Quest and Optum360, which the Court addresses in turn.

a. Affirmative Misrepresentations

An actionable misrepresentation under the MNCFA "must be a 'specific and measurable claim, capable of being proved false or of being reasonably interpreted as a statement of objective fact.'" Laughlin v. Target Corp., No. 12-489, 2012 WL 3065551, at *2 (D. Minn. July 27, 2012) (quoting Am. Italian Pasta Co. v. New World Pasta Co., 371 F.3d 387, 391 (8th Cir. 2004)). However, a plaintiff need not plead or prove that a misrepresentation was intentional. Johannessohn, 450 F. Supp. 3d at 952 (collecting cases).

[50] The Minn. CFA prohibits "[t]he act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby." Minn. Stat. § 325F.69, subd. 1.

Hollway attempts to establish a misrepresentation by alleging that she read and was exposed to statements in Quest's privacy policy prior to agreeing to obtain blood testing on specific dates. Quest CCAC ¶¶ 149, 480. Quest's privacy policy provides:

> We exercise great care to protect your personal information. This includes, among other things, using industry standard techniques such as firewalls, encryption, and intrusion detection. As a result, while we strive to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us or receive from us. This is especially true for information you transmit to us via email since we have no way of protecting that information until it reaches us since email does not have the security features that are built into our websites.
>
> In addition, we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information. We educate our employees about the importance of maintaining confidentiality of customer information."
>
> We will not disclose any personal information to any third party (excluding our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential) . . . ."

Id. ¶ 347 (emphasis added). But Hollway has failed to particularly allege what aspect of this policy was false or misleading.

Initially, the policy cannot be read as a guarantee of information security. It expressly states that Quest cannot ensure the security of information transmitted to it and that it may share information to contractors with a business reason for the information, such as payment collection. Quest's HIPAA Policy also explicitly states that Personal Information may be provided to "an outside collection agency to obtain payment when necessary." Quest CCAC ¶ 345. Plaintiff does not allege that Quest failed to otherwise limit access to Personal Information or that AMCA was not "obligated" to maintain confidentiality.

Further, Quest's vow to take "great care" to protect Personal Information is not an actionable representation. Indeed, it is unclear that this assertion can be considered a statement of

objective fact, as opposed to mere puffery. See, e.g., Laughlin, 2012 WL 3065551, at *2 ("Puffery exists in two general forms: (1) exaggerated statements of bluster or boast upon which no reasonable consumer would rely; and (2) vague or highly subjective claims of product superiority, including bald assertions of superiority.") (citation and quotation marks omitted). Courts have held that similarly vague statements related to data privacy cannot support a consumer fraud action because they "say[ ] nothing about the specific characteristics" of a defendant's services. See In re Yahoo!, 2017 WL 3727318, at *26 (holding that statement in privacy policy that "protecting . . . our users' information is paramount" was non-actionable puffery). The Court sees no workable standard by which to assess the falsity of Defendants' "great care," nor have plaintiffs provided the Court with one.

Hollway has therefore failed to allege an actionable misrepresentation.

b. Material Omissions

"For [a MNCFA] claim based on an omission, a plaintiff must prove an omission of material fact, as well as special circumstances that trigger a duty to disclose." Johannessohn, 450 F. Supp. 3d at 951 (citing Graphic Commc'ns Local 1B Health & Welfare Fund A v. CVS Caremark Corp., 850 N.W.2d 682, 696 (Minn. 2014)). Hollway alleges that Quest and Optum360 failed to disclose two material facts: (1) that they "did not reasonably or adequately secure . . . Personal Information or ensure its vendors and business associates reasonably or adequately secured such information," Quest CCAC ¶ 480(f); and (2) that they "did not comply with common law and statutory duties pertaining to Personal Information," id. ¶ 480(g).

The latter "omission" is not actionable, and the Court is unconvinced it can even coherently be called an omission. Defendants' alleged failure to disclose that they were violating state and

federal law concerns a legal conclusion, not an objective material fact. Plaintiffs cite no authority that would permit them to bootstrap violations of other law into a MNCFA claim.

On the other hand, courts have permitted omission-based consumer fraud claims to proceed where a Plaintiff alleges that a company failed to disclose that it "did not have reasonable or adequate safeguards in place to protect [Personal Information]." In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 991 (S.D. Cal. 2014) ("In re Sony II"); see also Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1251 (D. Colo. 2018) ("Plaintiffs assert that Defendant failed 'to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard [Personal Information]."); In re Adobe Sys., Inc. Priv. Litig., 66 F. Supp. 3d 1197, 1229-30 (N.D. Cal. 2014) (finding actionable omission of fact that defendant's "security practices fell short of industry standards").

The Court adopts the reasoning of these decisions, with one caveat—Hollway's alleged injuries were not caused by Defendants' own data security failures, but rather by their alleged failure to oversee AMCA's security practices. See, e.g., Quest CCAC ¶ 323 ("By failing to adequately monitor and audit the data security systems of their vendors and business associates, Quest put patient information at severe risk."). In the context of this case and the specific injuries claimed by Hollway, the only well-pled omission is Quest's alleged failure to disclose that it did not reasonably ensure that AMCA secured Personal Information.

With respect to a duty to disclose, Minnesota law imposes such duty on a "party to a transaction" in three circumstances: "(a) [o]ne who speaks must say enough to prevent his words from misleading the other party[;] (b) [o]ne who has special knowledge of material facts to which the other party does not have access may have a duty to disclose these facts to the other party[;] and (c) [o]ne who stands in a confidential or fiduciary relation to the other party to a transaction

must disclose material facts." Klein v. First Edina Nat. Bank, 196 N.W.2d 619, 622 (Minn. 1972). Plaintiff contends that Defendants had a duty to disclose based on their "special knowledge of material facts," specifically, "their lax data security practices with respect to sharing with third parties." Pl. Opp. to Quest Mot. at 46.

The Court can draw a reasonable inference from the CCAC that Defendants had exclusive knowledge of their own due diligence and oversight practices that were not publicly disclosed. This is sufficient to allege a duty to disclose with respect to Quest, with whom Plaintiff had a direct transactional relationship. For the reasons previously discussed however, no similar duty exists with respect to Optum360. See supra Section IV.D.1.b. Unlike Quest, Optum360 was not a "party to transaction," that may have a duty based solely on its exclusive knowledge of material facts.

Hollway has also sufficiently alleged causation and injury. She has pled economic injury in the form of fraudulent charges, along with time and money spent to remedy actual instances of identity theft. Quest CCAC ¶¶ 156-61. And unlike the vast majority of Plaintiffs, Hollway alleges that she read and agreed to Quest's privacy policy before deciding to purchase services, id. ¶ 149, meaning that had the omitted information been disclosed, she would have been aware of it. This satisfies Hollway's modest burden to plausibly allege that the omission "had some impact on" her purchasing decision. Johannessohn, 450 F. Supp. 3d at 951.

Finally, Hollway has alleged a public benefit. The MNCFA's public benefit requirement is "not onerous," Cleveland, 2021 WL 3173702, *8, and is satisfied whenever a plaintiff challenges deceptive conduct that targets "a significant segment of the public," Khoday v. Symantec Corp., 858 F. Supp. 2d 1004, 1017 (D. Minn. 2012) (citing Collins v. Minn. Sch. of Bus., Inc., 655 N.W.2d 320, 330 (Minn. 2003)). Here, a public benefit exists because Quest's alleged omissions

were made to its entire customer base, which allegedly encompasses "one in three adult Americans." Quest CCAC ¶ 302.

Hollway's MNCFA claim may proceed against Quest only. All other MNCFA claims asserted in the Quest CCAC are dismissed.

3. Minnesota Uniform Deceptive Trade Practices Act

Hollway also alleges that Quest and Optum360 violated the MNUDTPA's prohibition on "deceptive trade practices." Minn. Stat. Ann. § 325D.44, subd. 1. Defendants ask the Court to dismiss this claim because Hollway has failed to allege a redressable threat of future harm. The Court agrees.

"[T]he sole statutory remedy for deceptive trade practices [under the MNUDTPA] is injunctive relief." Superior Edge, Inc. v. Monsanto Co., 964 F. Supp. 2d 1017, 1041 (D. Minn. 2013). Thus, to state a MNUDTPA claim, a Plaintiff must plausibly allege a threat of future harm that can be remedied by injunction. See, e.g., Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 773 (C.D. Ill. 2020); see also Superior Edge, Inc., 964 F. Supp. 2d at 1041 ("[MN]UDTPA provides relief from future damage, not past damage."). "In most consumer actions, the plaintiff is unable to allege facts showing a likelihood of future harm because the harm has already occurred, and because the plaintiff is unlikely to be deceived by a defendant's misstatements again in the future." Perdue, 455 F. Supp. 3d at 773.[51]

While Hollway has alleged the threat of future identity theft, "this is not the type of harm that the Court is able to issue an injunction against." Perdue, 455 F. Supp. 3d at 773. An injunction

[51] The seemingly anomalous existence of a statute that permits consumer protection claims but rarely entitles a consumer to relief can be explained by the fact that the MNUDTPA broadly applies to all conduct "in the course of business, vocation, or occupation." Minn. Stat. Ann. § 325D.44, subd. 1. Future harm is more likely, for example, where a business seeks to enjoin a competitor's ongoing deceptive practices that harm the business. See, e.g., Johnson v. Bobcat Co., 175 F. Supp. 3d 1130, 1141 (D. Minn. 2016).

against Quest or Optum360 will not prevent hackers already in possession of Hollway's Personal Information from doing future harm. Moreover, Hollway alleges that she has now paid for the services rendered by Quest, Quest CCAC ¶¶ 152-53, meaning there is no danger of Quest providing her Personal Information to another third-party collections vendor with lax security protocols. Lastly, like many consumers seeking injunctive relief, Hollway alleges that she would not have used Quest if she had known it would not protect her Personal Information, rendering it "unlikely that [she] will be deceived again." Johnson, 175 F. Supp. 3d at 1141.

The Court thus dismisses Hollway's MNUDTPA claim for failure to allege future harm.

4. Florida Deceptive and Unfair Trade Practices Act

Quest Plaintiffs Benadom and N. Infield, LabCorp Plaintiffs T. Harris, Laufenberg, and Petri, and Sonic Plaintiff Anderson each assert claims under the FDUTPA. Defendants argue that each Plaintiffs' claims fail because they suffered no "actual damages" within the meaning of the statute and have not alleged a basis for injunctive relief. The Court agrees.

"[A] consumer claim for damages under FDUTPA has three elements: (1) a deceptive act or unfair practice; (2) causation; and (3) actual damages." Rollins, Inc., 951 So.2d at 860; see also Fla. Stat. Ann. §§ 501.204(1), 501.211(2). Courts have held that the failure to adequately secure Personal Information may qualify as an actionable "unfair practice" under the FDUTPA. See, e.g., In re Brinker, 2020 WL 691848, at *12 (citing Burrows v. Purchasing Power, LLC, No. 12-22800, 2012 WL 9391827, at *6 (S.D. Fla. Oct. 18, 2012)).

"Actual damages" under the FDUTPA is a term of art meaning "the difference in the market value of the product or service in the condition in which it was delivered and its market value in the condition in which it should have been delivered according to the contract of the parties." Carriuolo v. Gen. Motors Co., 823 F.3d 977, 986 (11th Cir. 2016) (citing Rollins, Inc. v.

Heller, 454 So.2d 580, 585 (Fla. Dist. Ct. App. 1984)). This is the FDUTPA's sole permissible measure of recovery—the statute expressly excludes claims for personal injury or consequential damages to any "property other than the property that is the subject of the consumer transaction." In re Brinker, 2020 WL 691848, at *13 (citing Fla. Stat. Ann. § 501.212(3)).

Plaintiffs allege that Defendants' conduct diminished the value of their Personal Information and resulted in a lost "benefit of the bargain" with respect to their purchase of services. In In re Brinker, Plaintiffs alleged that they overpaid for food at a restaurant and would have paid less had the defendant disclosed its inadequate data security. 2020 WL 691848, at *13. The Court held that for purposes of FDUTPA, the "property that is the subject of the consumer action" was food, not data security. The Court observed:

> In the same way that loan payments and interest are consequential costs of financing the purchase of a car . . . so to is data security for payment information in purchasing food at a restaurant using a credit card. . . . Ultimately, the food or drink purchased has no diminished value because of [defendant's] alleged inadequate data security; Plaintiffs' personal information is merely "other property[.]"

Id.

Here too, Plaintiffs have not alleged that Defendants' conduct reduced the value of "property that is the subject of the consumer action," here medical services. Additionally, Plaintiffs' allegations of fraudulent charges, expended time, purchase of monitoring services, and hacked accounts are unrecoverable "consequential damages." See, e.g., In re Brinker, 2020 WL 691848, at *13 (citations omitted) ("Plaintiffs have not alleged damages recognized under FDUTPA because unauthorized charges, lost time, and lost cash-back rewards are all consequential damages."); In re Sony II, 996 F. Supp. 2d at 994 (holding that FDUTPA did not permit recovery for interruption of services or lost premiums paid to third parties arising from data

breach). Though sufficient to confer Article III standing, these harms fail to satisfy the FDUTPA's more demanding "actual damage" requirement.

In the absence of actual damages, the FDUTPA permits any "aggrieved party" to pursue injunctive relief. Ahearn v. Mayo Clinic, 180 So. 3d 165, 171-73 (Fla. Dist. Ct. App. 2015); see also Fla. Stat. Ann. § 501.211(1). But "[a]lthough the FDUTPA allows a plaintiff to pursue injunctive relief even where the individual plaintiff will not benefit from an injunction, it cannot supplant Constitutional standing requirements. Article III of the Constitution requires that a plaintiff seeking injunctive relief allege a threat of future harm." Marjam Supply Co. of Fla., LLC v. Pliteq, Inc., No. 15-24363, 2018 WL 4932871, at *4 (S.D. Fla. Apr. 23, 2018). For the reasons discussed, supra Section IV.D.3, no Plaintiff has adequately alleged a threat of future harm. Like Hollway, none of the Florida Plaintiffs allege that they still owe money to Defendants.

All remaining FDUTPA claims are therefore dismissed for failure to plead actual damages or a threat of future harm.[52]

5. California Consumers Legal Remedies Act

Quest Plaintiff Vieyra and LabCorp Plaintiffs Nazemnikov and Lassiter bring claims under the CLRA. Only Vieyra has pled a valid claim.

The CLRA proscribes specifically enumerated practices by "any person in a transaction." Cal. Civ. Code § 1770(a). Plaintiffs allege violations of subsections 1770(a)(5) and 1770(a)(7), which each prohibit affirmative misrepresentations and material omissions where there is a duty to disclose.[53] See, e.g., Daugherty v. Am. Honda Motor Co., 51 Cal. Rptr. 3d 118, 126 (Cal. App.

---

[52] The Court's dismissal of Anderson's FDUTPA claim disposes of the last remaining cause of action against Sonic. The Court therefore grants Sonic's Motion in its entirety.

[53] A duty to disclose under the CLRA arises under any of four distinct circumstances: "(1) when the defendant is the plaintiff's fiduciary; (2) when the defendant has exclusive knowledge of material facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the

2006). A named plaintiff in a CLRA class action must allege both that she relied upon the unlawful conduct and that the unlawful conduct caused her injury. See, e.g., Mullins v. Premier Nutrition Corp., No. 13-1271, 2016 WL 3440600, at *3 (N.D. Cal. June 20, 2016) (citations omitted). To plead reliance on an omission, a plaintiff must allege that "had the omitted information been disclosed, one would have been aware of it and behaved differently." Ehrlich v. BMW of N. Am., LLC, 801 F. Supp. 2d 908, 916 (C.D. Cal. 2010) (citing Mirkin v. Wasserman, 858 P.2d 568 (Cal. 1993)). Unlike the FDUTPA, the CLRA broadly permits recovery for "any damage" resulting from an unlawful practice. "'[A]ny damage' . . . is not synonymous with 'actual damages' and may encompass harms other than pecuniary damages." Steroid Hormone Prod. Cases, 104 Cal. Rptr. 3d at 338.

The Court's analysis of Vieyra's CLRA claim parallels its assessment of Hollway's claim under the MNCFA. See supra Section IV.D.2. Like Hollway, and for the same reasons, Vieyra has failed to plead an actionable misrepresentation in Quest's privacy policy but sufficiently alleges that (a) Quest omitted the material fact that it failed to reasonably ensure that AMCA secured Personal Information, (b) Quest had a duty to disclose such fact due to its exclusive knowledge of its own practices, and (c) Optum360 lacked a duty to disclose because it was not a "person in a transaction" and had no prior relationship with Vieyra. Moreover, Vieyra has pled reliance through allegations that he read and agreed to Quest's privacy policy prior to agreeing to blood testing, Quest CCAC ¶ 24, and that he relied upon Quest's omissions, id. ¶ 538. From this, the Court may infer that had Quest disclosed its oversight practices, Vieyra "would have been aware of it and behaved differently." Ehrlich, 801 F. Supp. 2d at 916. Finally, Vieyra's allegations

---

defendant makes partial representations that are misleading because some other material fact has not been disclosed." Collins v. eMachines, Inc., 202 Cal. App. 4th 249, 255 (Cal. App. 2011).

of a fraudulent charge and remedial expenses, Quest CCAC ¶¶ 28-29, are sufficient under the CLRA's generous "any damage" standard. Vieyra has thus pled a valid CLRA claim against Quest.

The same cannot be said as to Nazemnikov and Lassiter. Unlike Vieyra, these plaintiffs do not allege that they read LabCorp's privacy policies before agreeing to blood testing. They have therefore failed to allege actual reliance on any misrepresentation or that they "would have been aware" of LabCorp's alleged omission had it been disclosed. See In re Yahoo!, 2017 WL 3727318, at *29-30 (holding that plaintiffs failed to allege actual reliance with respect to omissions in a privacy policy they never read).

Consequently, Vieyra's CLRA claim may proceed against Quest only, while Nazemnikov's and Lassiter's CLRA claims are dismissed for failure to plead reliance.

6. California Unfair Competition Law

Vieyra, Nazemnikov, and Lassiter also bring claims under the UCL. And again, only Vieyra's claim against Quest survives.

The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Courts have interpreted this language to provide three independent bases for recovery. First, "fraud" claims are interpreted "in tandem" with fraud claims under the CLRA. See In re Tropicana Orange Juice Mktg. & Sales Pracs. Litig., No. 11-7382, 2019 WL 2521958, at *7 (D.N.J. June 18, 2019) (collecting cases). A plaintiff must likewise plead "actual reliance" to state a claim. See, e.g, In re Yahoo!, 2017 WL 3727318, at *29. Second, the UCL's "'unlawful' prong borrows violations of other laws," including the CLRA. Klein v. Chevron U.S.A., Inc., 137 Cal. Rptr. 3d 293, 326-27 (Cal. App. 2012). Third, the standard governing "unfairness" claim is

unsettled, but courts typically permit such claims to proceed where one of three tests are satisfied.[54] See DeFrank v. Samsung Elecs. Am., Inc., No. 19-21401, 2020 WL 6269277, at *14 (D.N.J. Oct. 26, 2020).

Critically, a plaintiff may seek only restitution or injunctive relief under the UCL. See Korea Supply Co. v. Lockheed Martin Corp., 63 P.3d 937, 943 (Cal. 2003). A plaintiff may seek restitution to "compel a defendant to return money obtained through an unfair business practice to persons in interest from whom the property was taken." In re Sony I, 903 F. Supp. 2d at 970 (citing Trew v. Volvo Cars of N. Amer., No. 05-1379, 2006 WL 306904, at *2 (E.D. Cal. Feb. 8, 2006)). A plaintiff must show that the defendant benefited but need not necessarily demonstrate that it received money directly from the plaintiff. Id. And as discussed, a plaintiff seeking injunctive relief must allege redressable future harm. Rahman v. Mott's LLP, No. 13-3482, 2014 WL 5282106, at *5 (N.D. Cal. Oct. 15, 2014) (holding that both the UCL and Article III require a showing of future harm for injunctive relief).

For the same reasons expressed above with respect to the CLRA, Vieyra has alleged a UCL fraud claim against Quest, but not Optum360, while Nazemnikov and Lassiter have failed to plead reliance. Vieyra may also pursue an "unlawfulness" claim against Quest arising from the alleged CLRA violation. Moreover, Vieyra has adequately alleged grounds for restitution because he

[54] These tests are:

> (1) a "balancing test" considering the "reasons, justifications and motives of the alleged wrongdoer" compared to the practice's impact on its alleged victim, (2) a "competitor tethering test," where unfairness must be related to a legislatively declared policy or a threatened impact on competition, or (3) the test set out in section 5 of the Federal Trade Commission Act, which asks if the consumer injury is substantial, if the injury is outweighed by countervailing benefits, and if the consumers themselves could have reasonably avoided the injury.

DeFrank, 2020 WL 6269277, at *14 (citing Morgan v. AT&T Wireless Servs., Inc., 177 Cal. Rptr. 3d 768, 784-85 (Cal. Ct. App. 2009)).

conferred a benefit on Quest—payment for medical services—in reliance on Quest's alleged omission. Quest CCAC ¶¶ 22-23, 26.

To the extent Vieyra, Nazemnikov, and Lassiter bring claims for "unlawfulness" or "unfairness" arising from Quest's, Optum360's, or LabCorp's subsequent mishandling of Personal Information, they have failed to allege a basis for relief. Plaintiffs may not seek restitution for the alleged fraudulent charges and mitigation expenses they suffered because there was no corresponding benefit to Defendant. See, e.g., In re Sony I, 903 F. Supp. 2d at 970 (dismissing UCL claim for restitution because "Sony did not benefit financially from the Data Breach"). Plaintiffs have not alleged any benefit to Defendants beyond payment for testing services, see supra Section IV.C.3, and only Vieyra has adequately alleged that his purchase was caused by Quest's fraudulent and unlawful conduct. Lastly, no plaintiff has pled a likelihood of redressable future harm to justify injunctive relief. See supra Section IV.D.3.

In sum, Vieyra's UCL "fraud" and "unlawfulness" claim may proceed against Quest only. Nazemnikov's and Lassiter's fraud claims are dismissed for failure to plead reliance. All other UCL unlawfulness and unfairness claims are dismissed for failure to plead grounds for restitution or injunctive relief.

7. Massachusetts Consumer Protection Act

LabCorp Plaintiff Shulman brings a claim under the MACPA. Her claim may proceed.

The MACPA proscribes "deceptive" and "unfair" acts in the conduct of trade or commerce. Mass. Gen. Laws Ann. ch. 93A, § 2. To state a claim, a plaintiff must allege an "economic injury," Hanrahran, 54 F. Supp. 3d at 156, along with factual and proximate causation, see Walsh v. TelTech Sys., Inc., 821 F.3d 155, 160 (1st Cir. 2016).

Conduct is "deceptive" when "it has the capacity to mislead consumers, acting reasonably under the circumstances, to act differently than they otherwise would have acted." Hanrahran, 54 F. Supp. 3d at 154 (citing Aspinall v. Philip Morris Cos., Inc., 813 N.E.2d 476, 488 (Mass. 2004)). To determine whether conduct is "unfair," Massachusetts courts consider several factors: (1) whether the practice is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers[.]" Id. (citing Mass. Eye & Ear Infirmary, 552 F.3d at 69). Ultimately, however, the determination of whether a practice is "unfair" is reserved to the finder of fact. Id.

With respect to LabCorp's allegedly "deceptive" pre-purchase misrepresentations and omissions, to establish causation Shulman must allege that "had [LabCorp] been candid about [its] data security compliance, [her] losses would not have occurred." Ferreira v. Sterling Jewelers, Inc., 130 F. Supp. 3d 471, 484 (D. Mass. 2015). She has failed to do so. Shulman does not allege that she read LabCorp's data security policies and thus cannot show that her purchasing decision was caused by any disclosures or omissions made by LabCorp.

That said, Shulman may proceed on her "unfairness" claim. As under the FDUTPA, a failure of data security may qualify as an unfair practice under the MACPA, independently of any deceptive conduct. See, e.g., In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 498 (1st Cir. 2009) (reversing dismissal of MACPA claim "that defendants' lack of security measures was 'unfair'"). Shulman has adequately alleged that the Data Breach caused economic injuries in the form of fraudulent charges and mitigation expenditures. LabCorp CCAC ¶ 26. While Shulman

will ultimately need to demonstrate that these injuries have "economic" value, she need not do so at the pleading stage.[55]

8. Michigan Consumer Protection Act & Pennsylvania Unfair Trade Practices and Consumer Protection Law

Michigan resident Rutan asserts claims against Quest and Optum360 under the MICPA, while Quest Plaintiff Saracina and LabCorp Plaintiff Judelsohn assert claims under the PUTPCPL. Defendants contend that each claim fails for failure to plead reliance. The Court agrees.

The MICPA and PUTPCPL each proscribe a wide variety of specifically defined conduct. See Mich. Comp. Laws § 445.903; 73 Pa. Stat. Ann. § 201-2(4). Each statute requires a plaintiff to show actual reliance on the defendant's allegedly wrongful conduct to recover. See In re OnStar Cont. Litig., 278 F.R.D. 352, 376-78 (E.D. Mich. 2011) (MICPA);[56] In re Rutter's Inc. Data Sec. Breach Litig., 511 F. Supp. 3d at 542 (PUTPCL).

Plaintiffs allege violations of MICPA and PUTPCPL subsections that prohibit false representations and omissions of material fact. See Quest CCAC ¶¶ 658, 734; LabCorp CCAC ¶ 425. But neither Rutan, Saracina, nor Judelsohn have alleged that they viewed any data privacy policies before obtaining services from Quest or LabCorp. For the reasons discussed above, this prevents them from establishing actual reliance. The Court thus dismisses Plaintiffs' MICPA and PUTPCPL claims for failure to plead reliance.

---

[55] LabCorp argues that Shulman has failed to satisfy the statutory requirement that the alleged unlawful conduct "occurred primarily and substantially within [Massachusetts]." Mass. Gen. Laws ch. 93A, § 11. At this stage, the Court declines to dismiss Shulman's claim on this ground. Shulman alleges that she is a resident of Massachusetts, LabCorp CCAC ¶¶ 26, and that LabCorp sold services in Massachusetts, id. ¶ 350. Though Shulman does not expressly allege that she obtained services or provided her Personal Information in Massachusetts, it is reasonable to infer that Shulman received medical services in her home state. Cf. In re TJX, 564 F.3d at 498 (holding that data breach plaintiff alleged compliance with Mass. Gen. L. ch. 93A, § 11 because defendant had an office in Massachusetts and presumably communicated with servers in Massachusetts). To the extent LabCorp can demonstrate otherwise, it may renew its argument on summary judgment.

[56] Though the MICPA permits a class-wide inference of reliance without individual proof, a named plaintiff "must still allege actual reliance." In re Sony II, 996 F. Supp. 2d at 997.

9. New York General Business Law

Quest Plaintiffs Briley and Rosselli and LabCorp Plaintiffs Gadero and Lamondie-Murphy bring claims under the NYGBL. These Plaintiffs have failed to plausibly allege causation.

To state a claim under the NYGBL, a plaintiff must allege "(1) that the defendant's acts were consumer oriented, (2) that the acts or practices are deceptive or misleading in a material way, and (3) that the plaintiff has been injured as a result." Goldemberg, 8 F. Supp. 3d at 478 (citation and quotation marks omitted); see also N.Y. Gen. Bus. Law § 349. Though a plaintiff need not plead reliance, i.e., that he "would not otherwise have entered into the transaction," a consumer must still allege that he was aware of the deceptive conduct and was "personally misled" to satisfy the causation requirement. See Fero v. Excellus Health Plan, Inc., 502 F. Supp. 3d 724, 739-40 (W.D.N.Y. 2020) (collecting cases).

Like the Michigan and Pennsylvania Plaintiffs, neither Briley, Rosselli, Gadero, nor Lamondie-Murphy allege that they read any data privacy policies before purchasing medical services. They therefore cannot show that they were exposed to any misrepresentations or that they would have been aware of any alleged omissions, had they been disclosed. See id. at 740 ("[W]hile a plaintiff pursuing a GBL § 349 claim need not have relied on (or even necessarily have believed) the allegedly deceptive conduct, he or she must have at least been exposed to it.").

Moreover, to the extent Plaintiffs allege that Defendants' alleged oversight failures were an independent "deceptive or misleading" practice, the Court disagrees. Under the NYGBL, the phrase "deceptive acts or practices" means an "actual misrepresentation or omission to a consumer." Goshen v. Mut. Life Ins. Co. of N.Y., 774 N.E.2d 1190, 1195 (N.Y. 2002). In fact, a New York court in a related case has squarely held that a medical provider's "alleged failure to safeguard information on AMCA's networks did not mislead plaintiff in any material way and

does not constitute a deceptive practice within the meaning of [the GBL]." Smahaj v. Retrieval-Masters Creditors Bureau, Inc., 131 N.Y.S.3d 817, 827-28 (N.Y. Sup. Ct. 2020) (citation omitted).

The Court therefore dismisses Plaintiffs' NYGBL claims.

* * *

At bottom, only four consumer protection claims may proceed: (1) Hollway's MNCPA claim against Quest; (2) Vieyra's CLRA claim against Quest; (3) Vieyra's UCL claim against Quest; and (4) Shulman's MACPA claim against LabCorp. All other consumer protection claims are dismissed, for the reasons discussed above.

E. Cybersecurity and Data Breach Statutes

In addition to their statutory consumer protection claims, Plaintiffs bring 14 claims under the cybersecurity and data-breach statutes of 13 states. Eight such claims are brought only on behalf of plaintiffs without standing and will not be considered.[57] Moreover, Plaintiffs have withdrawn their claims under the Tennessee Personal Consumer Information Release Act. See Pl. Opp. to Quest Mot. at 51. Thus, only five statutory claims remain.[58]

Defendants argue that, for various reasons, the CCACs fail to state a viable claim under any state data-breach statute. The Court addresses each in turn.

---

[57] The Court will not consider claims under the following states' laws: (1) Colorado (Quest Plaintiff Perez), Quest CCAC ¶¶ 33, 542-49; (2) Connecticut (all CareCentrix Plaintiffs), CareCentrix CCAC ¶¶ 187-203; (3) Iowa (Quest Plaintiff Dirks), Quest CCAC ¶¶ 94, 581-91; (4) Kansas (Quest Plaintiff A. Finch and LabCorp Plaintiff D. Finch), id. ¶¶ 104, 603-10; LabCorp CCAC ¶¶ 22, 276-283; (5) Kentucky (Quest Plaintiffs Green and Perry and LabCorp Plaintiff Rothwell), Quest CCAC ¶¶ 118, 127, 627-634; LabCorp CCAC ¶¶ 23, 300-07; (6) Maryland (LabCorp Plaintiffs Jerry and Kaplan), LabCorp CCAC ¶¶ 24, 333-46; (7) New Hampshire (Quest Plaintiff Jaworowski), Quest CCAC ¶¶ 174, 674-681; and (8) Wisconsin (LabCorp Plaintiff Allende), LabCorp CCAC ¶¶ 42, 441-48.

[58] At least one plaintiff has standing to assert claims under the following statutes: (1) the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.101 ("CMIA"); (2) the California Customer Records Act, Cal. Civ. Code § 1798.81.5 ("CRA"); (3) the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. § 445.72 ("MITPA"); (4) the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. § 56:8-163 ("CSBDA"); and (5) the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §§ 75-60, et seq. ("NCITPA").

1. California Confidentiality of Medical Information Act

Defendants contend that the CMIA claims of Plaintiffs Vieyra, Lassiter, and Nazemnikov fail for several reasons, including that the CCACs fail to allege that "medical information," as contemplated by the CMIA, was stolen. The Court agrees.

The CMIA requires a healthcare provider or its contractor "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. The CMIA defines "medical information" as "individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor <u>regarding a patient's medical history, mental or physical condition, or treatment</u>." Cal. Civ. Code § 56.05 (emphasis added). Therefore, the text of the CMIA specifies, and California courts have recognized, that "medical information" must include "a patient's medical history, mental or physical condition, or treatment." <u>Eisenhower Med. Ctr. v. Superior Ct.</u>, 226 Cal. App. 4th 430, 434-35 (2014).

California courts have dismissed CMIA actions when the information allegedly wrongfully disclosed did not include the plaintiffs' "personal medical history, diagnoses, or care." <u>Doe I v. Sutter Health</u>, No. 34-2019-00258072, 2020 WL 1331948, at *4 (Cal. Super. Jan. 29, 2020). Here, Plaintiffs have not alleged any facts to show that such "medical information" was involved in the Data Breach. For example, Plaintiffs do not allege that laboratory test results or diagnostic information were in AMCA's affected system. <u>See, e.g.</u>, LabCorp CCAC ¶¶ 66, 84. While Plaintiffs do allege that the "Personal Information" impacted included "dates of service and referring doctor," <u>id.</u> ¶ 2, that information does not rise to the definition of "medical information" under California law. <u>See</u> <u>Eisenhower Med. Ctr.</u>, 226 Cal. App. 4th at 435-36 (fact that person

"was a patient" does not constitute medical information absent "substantive information regarding that person's medical condition, history, or treatment"). Simply, the information allegedly compromised (generally billing and collections-related information) is not the type of information protected by the CMIA. Thus, Plaintiffs wholly fail to allege that the Data Breach involved substantive medical information.[59] Absent factual allegations that the information compromised involved Plaintiffs' medical history and treatment programs, the CCACs fail to state a claim for relief under the CMIA.

2. California Customer Records Act

Next, Defendants argue that Plaintiffs' CRA claims fail because Defendants are categorically exempt from the CRA as a HIPAA-regulated entity. The Court agrees.

The CRA expressly excludes entities "governed by the medical privacy and security rules issued by the federal Department of Health and Human Services . . . pursuant to [HIPAA]." Cal. Civ. Code § 1798.81.5(e)(3). And the CCACs expressly allege that Defendants are HIPPA-regulated entities. See, e.g., LabCorp CCAC ¶¶ 130, 155; Quest CCAC ¶¶ 344, 419. Therefore, Defendants are exempted from the CRA, and Plaintiffs' CRA claims are dismissed with prejudice.

3. Michigan Identity Theft Prevention Act

Quest and Optum360 argue that a private plaintiff may not bring a claim under MITPA. The Court disagrees, but nonetheless concludes that Rutan's MITPA claim must be dismissed.

MITPA requires businesses to give notice of certain data security breaches "without unreasonable delay," but does not expressly provide a private right of action. Mich. Comp. Laws

[59] The CCAC against Quest and Optum360 defines "Personal Information" to include "diagnosis codes." Quest CCAC ¶ 4. However, the CCAC fails to explain what "diagnosis codes" are and what information they relay. The Court declines to read into this generalized allegation and infer from it that "medical information" was compromised in the Data Breach or that such information was downloaded, misused, or understood by third parties.

§ 445.72(1), (4). Instead, MITPA states only that its provisions allowing for public enforcement "do not affect the availability of any civil remedy for a violation of state or federal law." Id. § 445.72(15). Courts have interpreted this language to imply that a private plaintiff may seek recovery for a violation of MITPA, but only through the MICPA or "other laws." See, e.g., In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014); In re Equifax, 362 F. Supp. 3d at 1339.

Despite the general availability of a MITPA remedy through the MICPA, Rutan fails to allege such a claim here because reliance is an essential element of an MICPA claim. See supra Section IV.D.8. Rutan has failed to plead reliance on the allegedly inadequate notice, i.e., that had the notice been adequate, Rutan would have behaved differently. Nor has Rutan pointed to any "other law" through which he may assert a MITPA violation. The Court must therefore dismiss his MITPA claim.

4. New Jersey Customer Security Breach Disclosure Act

Quest and Optum360 raise similar arguments with respect to Jairam's claim under the CSBDA. Here, the Court concludes that Jairam has stated a valid claim, but only against Optum360.

A plaintiff may recover for a willful, knowing, or reckless violation of the CSBDA through the NJCFA. See N.J.S.A. § 56:8-166; see also Holmes v. Countrywide Fin. Corp., No. 08-205, 2012 WL 2873892, at *13 (W.D. Ky. July 12, 2012) (observing that the CSBDA provides no independent right of action); Equifax, 362 F. Supp. 3d at 1340-41 (permitting CSBDA claim to proceed via the NJCFA). Quest is exempt from the NJCFA as a "learned professional," see supra Section IV.D.1.a, and Jairam's CSBDA claim against Quest under the CSBDA is thus dismissed with prejudice.

With respect to Optum360, which is not necessarily exempt from the NJCFA, a willful violation of the CSBDA may provide the predicate "unlawful conduct" to support an NJCFA claim. N.J.S.A. § 56:8-166. The CSBDA requires a business that "compiles or maintains computerized records that include personal information," to disclose a security breach of those records to affected consumers "in the most expedient time possible and without unreasonable delay." N.J.S.A. § 56:8-163(a). The duty to disclose further extends to circumstances where an entity that maintains records "on behalf of" the business suffers a data breach and so-informs the business. Id. § 56:8-163(b).

Optum360 argues that it is not subject to the CSBDA because the CCAC fails to allege that it "compiles or maintains" Personal Information. The Court disagrees. Plaintiffs allege, among other things, that "Quest and/or Optum360 would provide AMCA with Quest patient's Personal Information which AMCA subsequently stored in its own computer systems." Quest CCAC ¶ 307. Thus, Jairam alleges that for however brief a time, Optum360 "compiled" and "maintained" Personal Information, and that AMCA held such information on Optum360's behalf. Jairam also alleges that Optum360's failure to expeditiously disclose the Data Breach was knowing, willful, or reckless, bringing her claim within the purview of the NJCFA. Id. ¶¶ 470(e), 472.

Jairam's CSBDA claim against Optum360 may therefore proceed.[60]

[60] The Court is satisfied that Jairam has otherwise pled a viable NJCFA claim arising from Optum360's alleged violation of the CSBDA. Any NJCFA claim must be supported by allegations of an "ascertainable loss" and a causal nexus between the defendant's unlawful conduct and the plaintiff's loss. Int'l Union of Operating Eng'rs Loc. No. 68 Welfare Fund, 192 N.J. at 389. Jairam has pled that she suffered an ascertainable loss in the amount of at least $2,000, Quest CCAC ¶ 189, and that Optum360's inadequate disclosure caused her damages, id. ¶ 697. Of course, Jairam must ultimately prove that her damages were caused by the delayed disclosure, and not simply by the Data Breach itself or some other factor. See, e.g., In re Sony II, 996 F. Supp. 2d at 1010.

5. North Carolina Identity Theft Protection Act

The parties agree that a private plaintiff may sue for a violation of the NCITPA but appear to disagree as to whether such claim must proceed through North Carolina's consumer protection statute. The Court holds that like the statutes of New Jersey and Michigan, any NCITPA claim must proceed through the NCUDTPA. Consequently, Vazquez's and Wrenn's claims against LabCorp are barred.

The NCITPA provides that "[a] violation of this section is a violation of [the NCUDTPA]. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation." N.C. Gen. Stat. Ann. § 75-65(i). The few courts to consider this language have determined that "a plaintiff must bring a claim for a violation of the NCITPA under the [NC]UDTPA." Rogers v. Keffer, Inc., 243 F. Supp. 3d 650, 662 (E.D.N.C. 2017); see also Patton v. Experian Data Corp., No. 17-1559, 2018 WL 6190349, at *11 (C.D. Cal. Jan. 23, 2018) (explaining that the NCITPA can be enforced through the NCUDTPA's remedial provisions). The plain language of the statute supports this construction. The NCITPA does not affirmatively provide an independent right of action, but merely states that (a) a plaintiff may enforce the NCITPA through the NCUDTPA; and (b) any plaintiff who otherwise has a private right of action, i.e., via the NCUDTPA, must demonstrate an injury stemming from an NCITPA violation to recover.

As LabCorp is a "learned professional" exempt from the NCUDTPA, see supra Section IV.D.1.a, Plaintiffs' NCITPA claims may not proceed and are dismissed with prejudice.

F. Declaratory Judgment

Finally, Defendants urge the Court to dismiss Plaintiffs' claims for declaratory judgment. The Court finds dismissal proper.

The Declaratory Judgment Act ("DJA") permits this Court to issue a declaratory judgment "[i]n a case of actual controversy." 28 U.S.C. § 2201(a).[61] The DJA does not create an independent cause of action, but rather a "remedy for existing cases or controversies." In re AZEK Bldg. Prod., Inc., Mktg. & Sales Pracs. Litig., 82 F. Supp. 3d 608, 624 (D.N.J. 2015). As a form of forward-looking relief, a plaintiff seeking a declaration must demonstrate, among other things, a threat of "real and immediate" future harm. Travelers Ins. Co. v. Obusek, 72 F.3d 1148, 1154 (3d Cir. 1995). A plaintiff must also show that a declaration would have some "practical utility" in resolving a fixed controversy between the parties. Wayne Land & Min. Grp. LLC v. Delaware River Basin Comm'n, 894 F.3d 509, 522 (3d Cir. 2018).

Here, Plaintiffs have failed to demonstrate a threat of future harm that could be remedied by a declaratory judgment. Plaintiffs' remaining claims principally allege that Defendants (a) breached common law and statutory duties to ensure that AMCA had adequate data security measures; (b) failed to disclose their lack of oversight over AMCA; and (c) failed to provide timely notice of the Data Breach. As an initial matter, Plaintiffs' request for a declaration regarding Defendants' own data security is unsupported by the allegations in the CCACs, none of which indicate that Defendants, as opposed to AMCA, have inadequate security or have ever experienced a significant breach themselves. For this reason, it is of no import that Defendants continue to possess Plaintiffs' Personal Information, see Quest CCAC ¶ 454, because there is no indication that this information will be inappropriately handled in the future. And as explained in Section IV.D.3, Plaintiffs have alleged no redressable future harm arising from Defendants' alleged lack of oversight or deficient pre-purchase disclosures.

[61] Although Plaintiffs do not specifically plead their claim under the DJA, federal law clearly applies to the procedural remedy that Plaintiffs seek. See W.R. Huff Asset Mgmt. Co. v. William Soroka 1989 Tr., No. 04-3093, 2009 WL 606152, at *2 (D.N.J. Mar. 9, 2009), as amended, 2009 WL 2436692 (D.N.J. Aug. 6, 2009).

For this reason, the Court dismisses Plaintiffs' claims for declaratory judgment.

V. CONCLUSION

For the reasons expressed above, Sonic's Motion to Dismiss, ECF No. 147, CareCentrix's Motion to Dismiss, ECF No. 176, and Inform's Motion to Dismiss, ECF No. 213, are **GRANTED**. LabCorp's Motion to Dismiss, ECF No. 148, Optum360's Motion to Dismiss, ECF No. 149, and Quest's Motion to Dismiss, ECF No. 150, are **GRANTED in part** and **DENIED in part**. The following claims may proceed:

1) The negligence and negligence per se claims of the following Plaintiffs against Quest and Optum360: Julio Antonio Perez Vieyra, Elizabeth Hollway, Ria Jairam, Ann Davis, Noel Benadom, Nancy Infield, Michael Rutan, John Briley, Joyce Rosselli, and Darlane Saracina;
2) The negligence and negligence per se claims of the following Plaintiffs against LabCorp: Sherrie Palmer, Sandra Lassiter, Aleksander Nazemnikov, Tanya Harris, Holly Laufenberg, Tatyana Shulman, Kristopher Thomas, Rosaria Gadero, and Melanie Vazquez, Timothy Petri, Valerie Scott, Cameron Spencer, Lori Lamondie-Murphy, Debra Wrenn, Edith Thrower, Timothy Judelsohn, and Tiffany Goins;
3) Elizabeth Hollway's claim against Quest under the Minnesota Consumer Fraud Act;
4) Julio Antonio Perez Vieyra's claims against Quest under the California Consumers Legal Remedies Act and the California Unfair Competition Law;
5) Tatyana Shulman's claim against LabCorp under the Massachusetts Consumer Protection Act; and
6) Ria Jairam's claim against Optum360 under the New Jersey Customer Security Breach Disclosure Act.

All other claims in the CCACs are **DISMISSED WITHOUT PREJUDICE** unless above indicated that dismissal is with prejudice. To the extent Plaintiffs can cure the deficiencies identified in this Opinion, they may file amended pleadings with sixty (60) days.

Date: December 16, 2021

/s/ ***Madeline Cox Arleo***
Hon. Madeline Cox Arleo
UNITED STATES DISTRICT JUDGE